




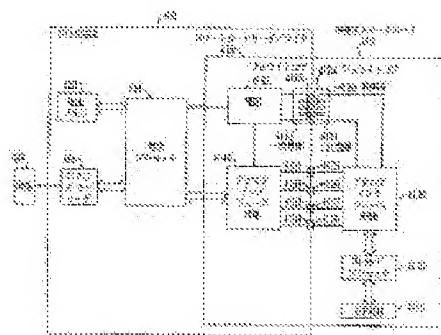


SMART CARD SYSTEM**Publication number:** JP7182426 (A)**Publication date:** 1995-07-21**Inventor(s):** UIRIAMU REIDO KAARURASURU; RIDEIA AN KAATEISU;
KIYASARIN EMU MAAFUII; RICHYAADO JIYON SUKIBO**Applicant(s):** AMERICAN TELEPHONE & TELEGRAPH**Classification:****- international:** **G06K19/00; G06Q10/00; G06Q30/00; G07F7/08; G07G1/14;**
G06K19/00; G06Q10/00; G06Q30/00; G07F7/08; G07G1/14;
(IPC1-7): G06F17/60; G06K19/00**- European:** G07F7/08C; G07F7/08C2C; G07G1/14B**Application number:** JP19940223942 19940826**Priority number(s):** US19930112487 19930827; US19940250144 19940527**Also published as:** EP0640945 (A2) EP0640945 (A3) BR9403345 (A) CA2117440 (A1) CA2117440 (C)**Abstract of JP 7182426 (A)**

PURPOSE: To enable a set of consumers to purchase commodities by drawing money from arbitrary one of plural accounts stored in a smart card. **CONSTITUTION:** A POS terminal 418 is provided with a terminal processor 424, a commodity discrimination device 426, a terminal memory 420, and a smart card reader 415. The commodity discrimination device 426 acquires a commodity identifier from a commodity to specify the commodity or its classification. A price table and plural commodity tables are electronically stored in the terminal memory 420, and each commodity identifier is related to a corresponding price. Each commodity table includes a list of commodity identifiers, and a specific commodity identifier is related to a corresponding account. Each commodity table is unequivocally discriminated by the commodity identifier. The terminal memory 429, the commodity discrimination device 426, and the smart card reader 415 are connected to a terminal processor.



Data supplied from the esp@cenet database — Worldwide

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平7-182426

(43)公開日 平成7年(1995)7月21日

(51)Int.Cl.⁶

識別記号

庁内整理番号

F I

技術表示箇所

G 0 6 F 17/60

G 0 6 K 19/00

G 0 6 F 15/ 21

3 4 0 A

G 0 6 K 19/ 00

U

審査請求 未請求 請求項の数12 F D (全 24 頁)

(21)出願番号 特願平6-223942

(22)出願日 平成6年(1994)8月26日

(31)優先権主張番号 1 1 2 4 8 7

(32)優先日 1993年8月27日

(33)優先権主張国 米国 (U S)

(31)優先権主張番号 2 5 0 1 4 4

(32)優先日 1994年5月27日

(33)優先権主張国 米国 (U S)

(71)出願人 390035493

エイ・ティ・アンド・ティ・コーポレーション

AT&T CORP.

アメリカ合衆国 10013-2412 ニューヨーク ニューヨーク アヴェニュー オブ
ジ アメリカズ 32

(72)発明者 ウィリアム レイド カールライスル

アメリカ合衆国、ニュージャージー、モリ
スタウン、マウント、ケンブル アベニュー
21

(74)代理人 弁理士 三俣 弘文

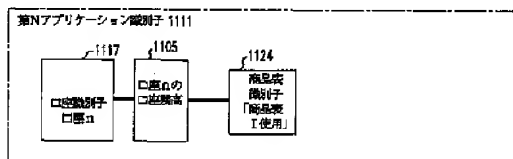
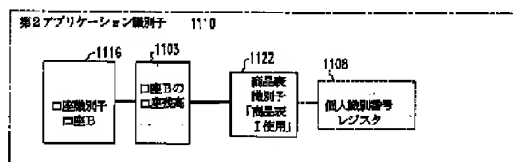
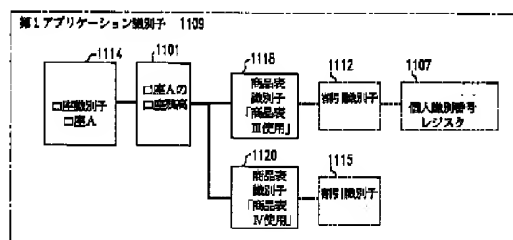
最終頁に続く

(54)【発明の名称】 スマートカードシステム

(57)【要約】 (修正有)

【目的】 スマートカード上に記憶された複数の口座のうち
の任意の口座から引き落としすることによって1組の消費者商品
を購入することを可能にする。

【構成】 POS端末は、端末プロセッサ、商品識別装置、
端末メモリ、及びスマートカードリーダを有する。商品識別装置
は、商品から商品識別子を取得し、商品又は商品の種別を特定
する。価格表及び複数の商品表が端末メモリに電子的に記憶さ
れ、各商品表は、商品識別子のリストを含み、特定の商品識別子
に対応する口座に関係づける。各商品表は、商品表識別子を使用
して一意的に識別される。端末メモリ、商品識別装置、及びス
マートカードリーダはすべて端末プロセッサに接続される。



【特許請求の範囲】

【請求項1】 特定の消費者商品または消費者商品の特定の種別を識別する商品識別手段と、端末メモリ手段と、前記端末メモリ手段および前記商品識別手段に接続された端末処理手段とを有するPOS端末と、スマートカードメモリ手段とスマートカード処理手段とを有するスマートカードとからなるスマートカードシステムにおいて、

前記スマートカードメモリ手段には、口座を一意的に指定する口座識別子と、その口座の残高を表す数値と、前記端末メモリ手段に格納された複数の商品表から商品表を一意的に識別する商品表識別子とを有する1つ以上のアプリケーション識別子をロードしたことを特徴とするスマートカードシステム。

【請求項2】 特定の消費者商品または消費者商品の特定の種別を識別する商品識別手段と、端末メモリ手段と、前記端末メモリ手段および前記商品識別手段に接続された端末処理手段とを有するPOS端末と、スマートカードメモリ手段とスマートカード処理手段とを有するスマートカードとからなるスマートカードシステムにおいて、

前記端末メモリ手段には複数の商品表がロードされ、各商品表は消費者商品のリストを含み、各商品表はその商品表に対応する商品表識別子によって一意的に識別されることを特徴とするスマートカードシステム。

【請求項3】 前記複数の商品表のうちの1つ以上が、特定の消費者の商品を特定の口座に関係づけることを特徴とする請求項1のシステム。

【請求項4】 前記複数の商品表のうちの1つ以上が、特定の消費者の商品を特定の口座に関係づけることを特徴とする請求項2のシステム。

【請求項5】 特定の消費者商品または消費者商品の特定の種別を識別する商品識別手段と、端末メモリ手段と、前記端末メモリ手段および前記商品識別手段に接続された端末処理手段とを有するPOS端末と、スマートカードメモリ手段とスマートカード処理手段とを有するスマートカードとからなるスマートカードシステムにおいて、

前記端末メモリ手段には複数の商品表がロードされ、各商品表は消費者商品のリストを含み、各商品表はその商品表に対応する商品表識別子によって一意的に識別され、

前記スマートカードメモリ手段には、口座を一意的に指定する口座識別子と、その口座の残高を表す数値と、前記端末メモリ手段に格納された複数の商品表から商品表を一意的に識別する商品表識別子とを有する1つ以上のアプリケーション識別子をロードしたことを特徴とするスマートカードシステム。

【請求項6】 前記商品表のうちの1つ以上が、特定の消費者の商品を特定の口座に関係づけることを特徴とす

る請求項5のシステム。

【請求項7】 複数のアプリケーション識別子をスマートカードにダウンロードするステップを有するスマートカードのプログラム方法において、各アプリケーション識別子は商品表識別子をスマートカードに格納された複数の口座のうちのいずれかに関係づけ、商品表は消費者商品のリストを含む商品表を一意的に指定することを特徴とするスマートカードのプログラム方法。

【請求項8】 複数の商品表をPOS端末にロードするステップを有することを特徴とするPOS端末のプログラム方法において、各商品表は消費者商品のリストと、商品表を一意的に識別する商品表識別子とを有することを特徴とするPOS端末のプログラム方法。

【請求項9】 スマートカードからPOS端末に商品表識別子をアップロードするステップをさらに有することを特徴とする請求項8の方法。

【請求項10】 消費者商品のリストを含む商品表を一意的に識別する商品表識別子を、スマートカードに格納された複数の口座のうちのいずれかにそれぞれ関係づける複数のアプリケーション識別子を格納する手段と、前記複数のアプリケーション識別子の1つ以上をPOS端末にアップロードする手段とを有することを特徴とするスマートカード。

【請求項11】 消費者商品のリストをそれぞれ有する複数の商品表を格納する手段と、前記複数の商品表のうちの特定の1つをそれぞれ一意的に識別する複数の商品表識別子を格納する手段とからなることを特徴とするPOS端末。

【請求項12】 スマートカードからPOS端末に商品表識別子をアップロードする手段をさらに有することを特徴とする請求項11のPOS端末。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、携帯型スマートカードに関し、特に、複数の銀行預金口座のうちの任意の口座から選択的に引き落としする機能を有するスマートカードを実現するシステムおよび方法に関する。

【0002】

【従来の技術】 マイクロエレクトロニクスにおける進展により、小さい空間内に多大な計算能力を備えることが可能となっている。実際、クレジットカード内に実質的にコンピュータ全体を入れることが可能となっており、これによって「スマートカード」が作成されている。スマートカードの大きな処理能力およびメモリ能力のために、スマートカードは従来のクレジットカードにとって代わり、代表的には、所定の口座から引き落としするカード保有者の権利を確認するために使用されることが期待されている。

【0003】

【発明が解決しようとする課題】 現在のスマートカード

のメモリは、複数のサービス提供者のプログラムおよびデータを保持するのに十分な大きさである。すなわち、単一のスマートカード上に、例えば、ビザ、マスターカード、ディスカバーおよびアメリカン・エクスプレスが共存するのに十分な大きさのメモリがある。しかし、現在のPOS環境では、従来のスマートカードが提供するのとは、1組の商品は単一の口座から引き落とすことによって支払をしなければならないような支払構造である。1組の商品を複数の口座から引き落とすことによって支払をすることを選択した場合、各口座に対して別々の引き落とし取引が必要となる。このようなシステムの例は、米国特許第4,816,653号(発明者:アンダー(Anders)他)および米国特許第4,837,422号(発明者:デスロフ(Dethloff)他)に記載されている。

【0004】現在のスマートカードシステムのもう1つの欠点は、複数のサービス提供者に対して金融取引を行うという問題に対する商業的に実現可能な解決法をもたないことである。この状況は、いくつかのセキュリティ問題が解決していないためであると考えられる。例えば、スマートカードのメモリ内のファイルについてカードの所有者およびこの所有者に与えられた権限に関して問題が生じる。商業的に言えば、他のサービス提供者が求めるセキュリティに一致しないスマートカードには、スマートカードの所有者(これもサービス提供者であることもある)はどの程度の権限を有するかという問題である。例えば、前掲のデスロフの米国特許に記載されたシステムでは、新たなサービス提供者がサービスをスマートカード上に提供することができるようになるためには、その前に、もとのサービス提供者がそのカードに追加情報を入力することを必要とする。この情報は、たとえ新たなサービス提供者がもとのサービス提供者とは別の口座を使用する場合でも、もとのサービス提供者によって入力されなければならない。このように、従来のシステムは競合するサービス間に商業的な衝突を生じ、このため、競合するサービスへの顧客のアクセスを制限したいという希望を提供者に対して助長することになっている。

【0005】

【課題を解決するための手段】スマートカード上に記憶された複数の口座のうちの任意の口座から引き落としすることによって1組の消費者商品を購入することが可能なシステムおよび方法を実現する。本発明の実施例によれば、POS端末は端末プロセッサ、商品識別装置、端末メモリ、およびスマートカードリーダを有する。商品識別装置は、複数の消費者商品のうちの任意の商品から商品識別子を取得する。この商品識別子は、商品または商品の種別を特定する。商品識別装置は、さまざまな消費者商品に取り付けられ、または、印刷された通常のUPCバーコードを読み取る通常のUPCバーコードリー

ダを有する。その代わりに、または、バーコードリーダに加えて、商品識別装置は、与えられた商品に対応するコードまたは記載をマニュアル入力するマニュアルデータ入力装置を有することも可能である。価格表および複数の商品表が端末メモリに電子的に記憶される。価格表は、各商品識別子に対応する価格に関係づける。各商品表は商品識別子のリストを含み、オプションとして、特定の商品識別子に対応する口座に関係づけることも可能である。各商品表は、商品表識別子を使用して一意的に識別される。端末メモリ、商品識別装置、およびスマートカードリーダはすべて端末プロセッサに接続される。

【0006】スマートカードには、複数のデータファイルを記憶するスマートカードメモリと、その複数のデータファイルを管理するソフトウェアオペレーティングシステムを実行するためのスマートカードプロセッサが装着されている。各データファイルは、口座を一意的に指定する口座識別子を、口座残高および1以上の商品表識別子と関係づける。口座は、例えば、ビザ、マスターカード、ディスカバー、ATMネットワーク、フードスタンプ(食券)プログラム、他の種類の福祉プログラム、失業補償、などのようなサービス提供者によって提供される。

【0007】任意に選択された複数の商品がPOS端末に提示され、1組の商品を構成する。端末プロセッサはスマートカードリーダを起動し、スマートカードメモリから端末プロセッサにデータファイルをアップロードする。スマートカードメモリからアップロードしたデータファイルに応答して、端末プロセッサは端末メモリから1以上の商品表を検索する。次に端末プロセッサは商品識別装置を起動する。各商品を識別するごとに、端末プロセッサは、その商品から取得される商品識別子を、端末メモリから検索した商品表にリストされた商品と比較する。商品識別子が商品表の商品に対応した場合、価格表でその商品識別子を検索し、その商品の価格または新たな口座残高を端末プロセッサからすかプロセッサにダウンロードすることによって、商品表によって指定される口座からその商品の価格を引き落とす。口座残高がスマートカードプロセッサにダウンロードされる場合、このステップは、1組の商品のうちの最後の商品が商品識別装置によって識別された後に実行することも可能である。この場合、商品価格は、前に端末プロセッサにアップロードされた口座残高から減算される。商品識別子が商品表のいずれの商品にも対応しない場合、その商品の価格を価格表から検索し、商品識別装置によって取得された商品識別子のうち商品表のいずれの商品にも対応しない商品識別子を有するすべての商品の価格を含む残余勘定に加えられる。商品識別装置によって取得された商品識別子が複数の商品表のうちに存在する場合、端末プロセッサによって引き落とし優先アルゴリズムが実行され、複数の商品表に対応する複数の口座の間で商品の価

格を割り当てる。1組の商品全体がPOS端末によって識別された後、残余勘定の全残高が、POS端末で、または、引き落とし優先アルゴリズムを実行することによって、選択された特定の口座に対応する口座残高から、引き落とされる。

【0008】

【実施例】POS環境でスマートカードに適用可能なシステムおよび方法の改良を図1～図14に示す。一般に、POS取引は以下のようにして行われる。カード保有者（すなわち消費者）は、購入する複数の消費者商品を選択し、スマートカードリーダを含むPOS装置に持ってくる。消費者商品はそれぞれ通常の統一商品コード（UPC）バーコード識別子を有する。これは、商品識別子として概念化することができる。消費者はスマートカードをスマートカードリーダに挿入することにより、複数の口座からの引き落としの動作のシーケンスを起動する。この動作シーケンスは以下の機能を実行する。購入する消費者商品の統一商品コード（UPC）、すなわち、商品識別子は、例えば、その商品のバーコードをスキャンすることによって、または、POS端末のキーパッドにコードをマニュアル入力することによって、商品識別装置により読み取られる。UPCコードおよびスマートカード上に保持されている1以上のアプリケーション識別子に基づいて、POS端末は、そのUPCを、メモリに記憶されている商品表と比較する。商品表は、カード保有者の1以上の口座に対するその商品の引き落としの適格性を識別する。商品が複数の口座に適格である場合、引き落とし優先アルゴリズムが、どの口座から引き落とすべきかを決定する。引き落とし優先アルゴリズムは1以上の引き落とし割当表を利用する。この表は、複数の商品識別子のそれぞれに対して、複数の口座の優先順位を示す。購入商品の商品UPCコードと、商品配列に記憶されたUPCコードとの比較は、各商品のUPCコードがPOS端末に入力されるときに行うことができる。その代わりに、各商品のUPCコードは、与えられたPOS取引のすべての商品が入力されるまでバッファリングすることも可能である。次に、各商品はそれぞれ口座から引き落とされる。さらに、カード保有者は、複数の口座に対応する単一の取引に対して単一のカード上で口座残高種別（ドル、特定商品識別、商品数量、など）を混合することができる。以上述べた機能は後で詳細に説明する。まず、スマートカードのソフトウェアオペレーティングシステムについて考える。

【0009】図1を参照すれば、本発明の特徴は、階層的ソフトウェアオペレーティングシステムの利用によって実現される。このようなオペレーティングシステムでは、サービス提供者またはスマートカードの所有者が、事前に許可なく、既存の各サービス提供者のためにまたは既存の各サービス提供者によって作成されたファイルにアクセスすることなく、異なるサービス提供者がスマ

ートカード上で共存することを可能にすべきである。

【0010】スマートカードのオペレーティングシステムは、UNIX（UNIXシステム・ラボラトリーの登録商標）にやや似ており、スマートカードの発行者／所有者によって所有される「ルート」（一次ソース）ディレクトリを有し、各サービス提供者は発行者／所有者によってインストールされる「ユーザ」である。このような各ユーザには、「ルート」（一次ソース）ディレクトリのサブディレクトリが与えられ、そのサブディレクトリ内にユーザはファイルおよびファイルを含むサブディレクトリを、ユーザが必要とするだけ作成する。

【0011】オペレーティングシステムは、スマートカードの発行者／所有者およびスマートカードの保有者を含むスマートカードの全ユーザに対して、ユーザが、所有するファイルに他のユーザからアクセスできないようにすることを選択した場合に、そのようなアクセスができないようにする。この排他能力は、ユーザによって所有され、スマートカードの発行者／所有者を含む他のユーザは変更できないパスワードファイルによって実現される。オプションとして、スマートカードの発行者／所有者には、与えられたユーザのすべてのファイルを消去する能力が与えられる。

【0012】また、オペレーティングシステムは、デジタル署名つき通信手段と、完全暗号化通信手段とを有する。この機能は、リモート通信における信頼性を与える。リモート通信により、リモート発給と、各スマートカードに含まれるすべてのサービスを追跡するデータベースの効果的な保守と、スマートカードの紛失または一般的故障の場合のスマートカードの再発給とが可能となる。

【0013】いくつかのスマートカードオペレーティングシステムが既に知られている。1つの例は、前掲のアンダー他の米国特許に記載されている。以下で説明するオペレーティングシステムは、そのオペレーティングシステムおよび周知のUNIXオペレーティングシステムと多くの類似点を有する。ここで説明するスマートカードオペレーティングシステムの理解を助けるため、UNIXオペレーティングシステムのいくつかの周知の事項を簡単に説明しておく。

【0014】[UNIXオペレーティングシステム] UNIXオペレーティングシステムはファイルの集合からなる。ファイルのうちのいくつかは、関連するファイルに関する情報を主に含み、ディレクトリファイルまたはディレクトリと呼ばれる。他のファイルはユーザデータを含み、「通常」ファイルという。また、UNIXオペレーティングシステムでは、ユーザは、ファイルの「owner（所有者）」であるか、ファイルによって認識される指定された「group（グループ）」に属するか、または、「other」に属することができる。各ファイルは、所有権、3種類のユーザに関する情報アク

セス能力などのようなファイル特徴を指定するデータ部分を含む。ファイルの所有者はすべてのファイル特徴を変更することができる。

【0015】構造的には、最初のファイルは「ルート」（一次ソース）ディレクトリファイルである。このディレクトリの所有者であるユーザは、実際、スマートカード全体の所有者である。このユーザは「ルート」（一次ソース）ファイルによって指される他のファイルを作成することができる。そのファイルは、他の「ディレクトリ」ファイルであることも「通常」ファイルであることも可能であり、ツリー上（階層）構造において「ルート」（一次ソース）ディレクトリの「下」にあるとみなされる。

【0016】多くのUNIXオペレーティングシステムでは、「ルート」（一次ソース）の下のディレクトリのうちの1つは「etc」と命名され、このディレクトリはその下に「passwd」というファイルを有する。このファイルの全アドレスすなわちパス名は「/etc/passwd」である（パス名の最初のファイル「/」は「ルート」（一次ソース）アドレスを表す）。「etc」および「passwd」ファイルは、一般に「ルート」（一次ソース）と呼ばれ「ルート」（一次ソース）ディレクトリの所有者でもあるシステム管理者によって所有される。「passwd」ファイルは「ルート」（一次ソース）のパスワードの暗号化表現を含み、オペレーティングシステムへの「ルート」（一次ソース）のアクセスは「ルート」（一次ソース）がパスワードを提示することによってログインした後でのみ許される。提示されるパスワードは暗号化され、「passwd」ファイルに格納された暗号化パスワードと比較される。比較が成功した場合、ユーザは認められ、他のファイルへのアクセスを許可される。すなわち、このユーザは「ログイン」したことになる。

【0017】「ルート」（一次ソース）が、「ルート」（一次ソース）ディレクトリ（または「ルート」（一次ソース）の下のサブディレクトリ）の下にサブディレクトリを作成し、そのサブディレクトリの所有権を他のユーザに割り当てることにより、マルチユーザ機能を実現することができる。次に、「ルート」（一次ソース）は、「passwd」ファイル内にそのユーザのパスワードをインストールし、そのユーザがそのパスワードを提示したときにそのサブディレクトリファイルにおいてシステムに入ることを可能にする。このユーザは自己のパスワードを変更する能力を有するが、それはオペレーティングシステムによって提供されるコマンドを通じてのみ可能である。そのパスワードは、システムにおいて、暗号化された形式でのみ、かつ、「passwd」ファイル内にのみ存在する。このアーキテクチャを図1に示す。

【0018】ログインプロセスは次のように要約するこ

とができる。UNIXオペレーティングシステムのもとで動作するコンピュータは、コンピュータの入力ポートをスキャンするループを実行することによって始動する。ユーザによる接続が検出されると、制御は、そのループからそのユーザとの対話を開始したプログラムに移る。そのプログラムは「login:」メッセージをユーザに送り、ユーザの応答を待つ。ユーザが（例えばストリング「htb」を返すことによって）自己を表示し、これが、そのユーザをオペレーティングシステムに対して識別させる。次に、プログラムは、要求メッセージ「Password:」を出し、ユーザはパスワードストリングを提示しなければならない。プログラムはそのパスワードストリングを暗号化し、それを、「/etc/passwd」ファイル内にあるその識別したユーザの暗号化パスワードと比較する。一致した場合、ユーザは真正である（確認された）と判定され、制御は「ルート」（一次ソース）によって所有されるファイル（代表的には、「profile」と命名されている）に渡される。このファイルはそのユーザに対してさまざまなパラメータを設定し、制御を、ユーザによって所有されるもう1つのファイル（代表的にはこれも「profile」と命名されるが、このファイルはそのユーザによって所有されるディレクトリ内にある）に渡される。そのユーザの「profile」内にある命令が実行された後、コンピュータはもう1つのループに入り、ユーザからの次の命令を待つ。

【0019】「ルート」（一次ソース）は、「passwd」ファイルを含めて、オペレーティングシステムを構成するすべてのファイルの所有者である。従って、「ルート」（一次ソース）は、任意のファイルを変更することが可能であり、従って「スーパーユーザ」である。「ルート」（一次ソース）によって所有されていないファイルであっても、「ルート」（一次ソース）のコマンドに従うことが重要である。「ルート」（一次ソース）にすべてのファイルの実質的な所有権を与えることは、ファイルが正式には他のユーザによって所有されている場合であっても、十分意味をなす。それは、「ルート」（一次ソース）が、「passwd」ファイルとともに、「ルート」（一次ソース）の能力を制御するファイルをも一般的に変更する能力を有するためである。このため、「ルート」（一次ソース）はパスワードを変更する能力を有し、従って、「ルート」（一次ソース）は常にファイルの所有者になることができる。従って、「ルート」（一次ソース）に所有者のすべての能力を直接持たせることは意味がある。簡潔に言えば、「ルート」（一次ソース）は、システム内のすべてのファイルの絶対的制御および全情報を有する。

【0020】（正確なパスワードを提示することによって）ログインすることができることに加えて、ユーザには、ファイルの読み出し、ファイルへの書き込み、ファ

イルの実行（すなわち、プログラム制御をファイルに渡すこと）の能力が与えられる。指定したファイルにプログラム制御を渡す能力がなければ、何も行うことができない。プログラムを実行することは、制御をファイルに渡すことにはかならないからである。「ルート」（一次ソース）はシステムのすべてのファイルにアクセスすることができるため、「ルート」（一次ソース）はすべてのファイルを読み出し、書き込み、実行することができる。

【0021】UNIXオペレーティングシステムのすべての命令は、単に実行可能なファイルであり、これらのファイルは、そのファイルがどこにあるかをシステムが知っている限り、どのディレクトリにも存在することができる。「ルート」（一次ソース）はそのようなすべてのディレクトリおよびファイルを所有する。「ルート」（一次ソース）はそれらのすべてのディレクトリおよびファイルの読み出しおよび実行の許可を制御するため、「ルート」（一次ソース）は、任意のユーザ（必要な場合には、自分自身を含めて）が、任意のファイルを実行しないように制限することが可能であり、これにより、
20 「ルート」（一次ソース）は、ユーザの特定のグループによる実行が制限されたファイルのカスタム化したセットを作成することができる。換言すれば、「ルート」（一次ソース）は、システムで利用可能なすべてのコマンドより少ないコマンドを含む、さまざまな制限されたオペレーティングシステム、すなわち、「制限シェル」を作成することができる。

【0022】[スマートカードオペレーティングシステム] UNIXオペレーティングシステムで「ルート」（一次ソース）が有する絶対的な能力は、スマートカードには不適當である。明らかに、ビザ、マスターカード、およびアメリカン・エクスプレスのような提供者は相互に「ルート」（一次ソース）であることを許容しないであろうが、明白に十分なセキュリティ手段がなければ、それら以外の第三者が「ルート」（一次ソース）となることも望まないと考えられる。このため、スマートカードは、あまり商業的成功を収めないことになる。

【0023】図2に、このサービス提供者の敏感さに対応する構造を示す。図2の構造によれば、「ルート」（一次ソース）は、「ルート」（一次ソース）ディレクトリおよび作成したい任意の数のファイル（ディレクトリファイルまたは通常ファイル）を所有する。例えば、図2は、「ルート」（一次ソース）ディレクトリファイル10を含み、その下には、「profile」ファイル11、「passwd」ファイル12、「log」ファイル17、「filex」ファイル13、「filey」ファイル14、および「ID」ファイル18がある。「ルート」（一次ソース）の下にはいくつかのサブディレクトリも存在し、それぞれユーザ（サービス提供者）の「HOME」ディレクトリとして使用され、ま
50

た、そのような各ユーザHOMEディレクトリに対してパスワードファイルが作成される。例えば、図2は、「htb」という名前（スマートカードの所有者）のディレクトリファイル15、「bankA」という名前のディレクトリファイル20、および、「airlineA」という名前のディレクトリファイル25を含む。各ディレクトリは、対応するユーザのHOMEディレクトリの下に、「passwd」ファイル（それぞれ16、21、および26）と、「profile」ファイルを含む。パスワードファイルのこの配置はいくつかの利点を有するが、これは必須ではない。重要なことは、このような各パスワードファイルの所有権はそのファイルおよびそのうえのディレクトリに対応するユーザに割り当てられることである。ファイル（ディレクトリ）15、20および25の所有権を各ユーザに与えることも有益である。

【0024】図2は、もう1つの重要なディレクトリ（およびユーザ）を含む。それは、「Visitor」ディレクトリ30であり、これは、スマートカードと対話したい非サービス提供者のエントリーポイントである。

【0025】図2のファイルアーキテクチャは、UNIXオペレーティングシステムとは異なるオペレーティングシステムと結合される。図2の構造のオペレーティングシステムは、主に、そのオペレーティングシステムでは「ルート」（一次ソース）が所有しないファイルを変更する能力が「ルート」（一次ソース）には与えられないという点でUNIXオペレーティングシステムとは異なる。この機能が「ルート」（一次ソース）によって迂回されないことを保証するために、このオペレーティングシステムでは、「ルート」（一次ソース）が、オペレーティングシステムを定義するいくつかのファイルを変更することを許容しない（ある意味では、「ルート」（一次ソース）はそれらのファイルを所有しない）。この結果を実現する1つの手段は、それらの（非「ルート」（一次ソース）所有オペレーティングシステム）ファイルを読み出し専用メモリ（ROM）に格納することである。少なくとも、このROMは、ファイルへの書き込み（上書きまたは追加）を行うコマンド／モジュール／ファイルを含む。特に、ファイルへの書き込みは、ファイルの所有者が指定したものに制限され（ファイルの所有者は、最初は、そのファイルを作成したユーザである）、「ルート」（一次ソース）は単に他のユーザとして扱われる。ファイルへの書き込みを行うコマンドは、例えば、ファイルの移動、ファイルのコピー、ファイルの保存、ファイル属性（例えば所有権）の変更、およびファイル名の変更のようなオペレーティングシステムコマンドである。（各スマートカードに固有であるため）ROM（さらに一般的には「一回書き込み」メモリ）にインストールされる他の事項は、「ルート」（一次ソース）パスワードおよびスマートカードのID情報（すな

わち、ファイル12および18)である。ID情報は、単に任意のストリングであることも、保有者の名前を含むことも可能である(後者は、おそらく、ID情報を得た商人によって参照される)。実際には、「ルート」(一次ソース)パスワードおよびスマートカードのPINはいずれも「ルート」(一次ソース)ディレクトリを構成するファイルに格納することが可能である。図2では、説明のために、これらは独立のファイルとなっている。

【0026】スマートカードオペレーティングシステム10のいくつかの実施例では、1つのファイル書き込み能力が「ルート」(一次ソース)に与えられ、これは、任意のファイルを全体として削除する能力である(そして、そのプロセスで、実質的には、削除されたファイルが指しているファイルを削除する)。これには、ディレクトリファイルおよび通常ファイルが含まれ、「ルート」(一次ソース)が所有するファイルにも「ルート」(一次ソース)が所有しないファイルにも適用される。このような能力は、与えられたサービス提供者がスマートカードの保有者にもはやサービスを提供していないときにメモリ空間が再使用されるような実施例で与えられることが可能である。

【0027】図2のオペレーティングシステムと標準的なUNIXオペレーティングシステムのもう1つの相違点は、前者が、「ルート」(一次ソース)によって所有されるファイルに(例えば「filex」13に)インストールされた暗号キー対を含み、このキー対は各スマートカードに固有であるという点である。この対は、スマートカードによって秘密に保持される私的キーfと、スマートカードが秘密に保持するようには注意しない公開キーgとを含む。もちろん、両方のキーは、スマートカードの「ルート」(一次ソース)ユーザ(すなわち、スーパーユーザ)でもあるスマートカードの所有者/発行者には最初から既知であるが、「ルート」(一次ソース)は私的キーを保持する必要はない(そしておそらくその情報を破壊することを選択することになる)。このキー対は「ルート」(一次ソース)のパスワードを含むメモリのような適当なメモリに「焼き付けられ」、または、「ルート」(一次ソース)ディレクトリを定義するファイルに含められることも可能である。公開キー暗号化については後でさらに詳細に説明する。

【0028】ユーザのディレクトリのパスワードがそのユーザによって所有されるファイルに格納されるということは、UNIXオペレーティングシステムと図2のオペレーティングシステムの重要な相違点である。書き込みに対する制限とともにこの構成によって、「ルート」(一次ソース)は任意のファイル(通常ファイルまたはディレクトリファイル)の所有者になることはできなくなり、従って、「ルート」(一次ソース)はファイルの所有者によって設定された許可を迂回することができな

くなる。この重要な相違点によって、あるユーザのファイルは、スマートカードにアクセス可能な「ルート」(一次ソース)および他のユーザに対して完全に不透明となる。このようにして、図2の構成は、サービスの提供者とスマートカードの発行者/所有者の間の「信頼問題」を克服する。

【0029】[取引セキュリティ]解決すべき次の問題はスマートカードの取引セキュリティである。この概念は、スマートカードの保有者またはサービス提供者に悪影響を及ぼすような無許可の取引が起こらないことを保証するために、スマートカードのオペレーティングシステムによって、および、通信プロトコルに同意した者によって、使用される手段を含む。これは、「ルート」(一次ソース)、保有者、サービス提供者、ビジター(Visitor)ユーザ、または侵入者による活動を含む。(侵入者とは、スマートカードと他者の間の通信セッションに介入し、自己のメッセージを真のメッセージと置き換える者のことである。)

【0030】侵入者に対抗する1つの方法は、日付および時刻のタイムスタンプを含むメッセージを構成し、メッセージの少なくともその部分を暗号化することである。また、必要な場合には、通信プロトコルが、確認シーケンス(これはセッションごとに異なる)を当事者間で交換することを要求することも可能である。また、パスワードのような微妙な情報の明文で(すなわち、暗号化なしで)のフローを最小にするのも有効な一般的方法である。これらの技術は、後述のログインおよび通信プロトコルで使用される。

【0031】[暗号化]暗号化の分野は新しくない。以下の説明は、単に、本発明のスマートカードに関連して使用可能な2つの暗号化方式の要約である。

【0032】周知のように、暗号化のための「秘密共有」方式は、2つの通信者が秘密の関数fを共有することを要求する。メッセージmを送信したいほうの側は、その秘密関数でそのメッセージを暗号化して暗号化メッセージf(m)を形成する。この暗号化メッセージは送信され、受信側は関数f(f(m))を形成することによって受信した信号を復号する。関数fは、f(m)からメッセージmを発見することが計算量的に非常に困難であるが、その関数を2回適用することによってもとのメッセージが復元されるような関数(すなわち、f(f(m))=m)である。

【0033】暗号化のための「秘密共有」方式は非常に有効であるが、その弱点は、秘密関数を通信する(すなわち、共有する)必要があることである。その関数が伝送されているときの稀な通信セッション中にその共有の秘密が傍受者によって取得されてしまうと、もはやそれは秘密ではなくなる。

【0034】公開キー暗号化では、各当事者はキーの対fおよびgのうちの一方を保持する。すなわち、一方の

当事者が一方のキー（f）を秘密に保持し、それを通信することはないが、他方のキー（g）は、他方の当事者を含めてすべての者に知らせる（従って、キーgは「公開される」）。対fおよびgは次の3条件を満たすようなものである。

1. $g(f(m)) = m$ 。
2. gが既知である場合でも関数fは決定することができない。
3. f(m) からメッセージmを決定することは計算量的に実現不可能である。

【0035】公開キー方式は、前述のキー分配／管理の問題を解決するが、この方法は1つの欠点を有する。それは、公開キーの暗号化および復号が共有キー方式よりも遅い（より多くの計算時間を必要とする）ということである。

【0036】スマートカードに関しては、通信速度は、スマートカードと通信している当事者の種類に基づいて、異なる重要度を有する。スマートカードの発行者／所有者およびサービス提供者に関しては、通信は稀であることが予想され、従って、処理時間は「最重要」ではないため、低速度は主要な欠点ではない。しかし、それ以外の者（すなわち、ビジターユーザとしてログインする商人）との通信では、速度は重要である。

【0037】速度の問題は、必要であれば、「共有秘密」方式を公開キー方式と組み合わせることによって解決される。すなわち、通信を開始するとき、公開キー方式を使用して一時的な「共有秘密」をスマートカードと商人の間で通信する。特に、公開キーを有する側は「共有秘密」を提示し、それを、私的キーを有する側へ通信する。その後、より高速に、「共有秘密」方式を使用して全メッセージを暗号化する。

【0038】あるいは、（共有秘密を用いて）認証方式を使用することも可能である。認証方式では、メッセージは明文で送信され、「デジタル署名」が追加される（すなわち、「署名される」）。「デジタル署名」は、符号化されるメッセージのハッシング（例えば、ある数を法としての、メッセージ内の文字のASCIIコードの加算）である。もちろん、侵入者が真のデータを偽データで置き換えることができないことが保証されるようなアプリケーションでは、（おそらくは、公開キーを使用した確認プロセスの後で）情報は明文で送ることができる。

【0039】公開キー方式の使用は、キー管理のほとんどの問題を解決する。スマートカードと通信したい当事者の公開キーの初期情報の問題がなお残るが、スマートカード自体がその情報を提供することができるので、それは問題ではない。

【0040】「ルート」（一次ソース）によるログインおよびサービス提供者／ユーザのインストール暗号化が安全な通信を保証するため、スマートカードの発行

者／所有者はサービスのリモートインストールを信頼することができる。もちろん、発行者／所有者（すなわち、「ルート」（一次ソース））は、最初に、スマートカードにログインしなければならない。ログインのためのプロトコルを図3に示す。また、サービスインストールプロセスのためのプロトコルを図4に示す。

【0041】図3に示したように、プロセスは、スマートカードの所持者（P）がスマートカード（S）の真正な保有者として認証されることから開始する。この方式は、PIN（個人識別番号）を捕捉する可能性のある装置に所持者のPINストリングを通信しないことが好ましいような実施例で特に有用である。例えば、PおよびSが商人の構内に存在するようなアプリケーションでは、商人の装置は、電池で動作し、キーボード入力手段およびディスプレイ出力手段を有し、他のポートや書き込み可能メモリを有しないことが確認された、スタンドアロン型の装置とすることが可能である。動作時に、PはSをこのスタンドアロン装置に挿入し、キーボードでPINを入力し、正しければその装置のディスプレイはメッセージ「OK」を出力する。このことは、取引に使用した装置が何らかの将来の不正使用のために保有者のPINストリングを捕捉することがないというもう1つの意味でのセキュリティを保有者に与える。このようなスタンドアロン装置が利用可能でない場合（または、例えば所持者の家庭で「ダム」カードリーダーを使用するときのように通信がリモートである場合）、提示されるPINはカード内で処理されるべきであり、スマートカードからの「OK」メッセージは「タイムスタンプ」され、暗号化されるべきである。このことは、適当な暗号化キーが確立され日付および時刻の情報がSに伝えられた後まで、PがHとして確認されることは延期されなければならないことを示唆する。

【0042】図3に戻って、Hの真正な地位が確立された後、Sは自己を表示し、ログイン中のユーザが正当なユーザであることを確認する。特に、図3のプロトコルは次のように進行する。

【0043】a. Sは入力を促し、PはPINストリングを提示する。スマートカード内では、PINは、保有者が変更するためにオープンされた「ルート」（一次ソース）所有のファイル（例えば、図2のファイル14）内に存在する。Sは、提示されたPINストリングを、格納されているPINストリングと比較し、一致すれば、PはHとして確認されたことになる。

【0044】b. Hが確認されると、SとOの間の通信に注意を向けることができる。Sは、そのID番号と、ランダムストリングの形式でのパスワードチャレンジRND1とをOに提示することによって自己を表示する。

【0045】c. OはOのパスワードでRND1を暗号化してストリングK1（RND1）を形成し、それをSに返す。このパスワード応答の形式は明白にセッション

とに変化し、Oの真のパスワードが侵入者によって盗まれないことを保証する。Oが所有するすべてのスマートカードのパスワードをどこに保持し、このようなデータベースはどのくらい安全かという問題が残っている。しかし、実際にはOはパスワードのデータベースを保持する必要はない。Oに必要なのは、Sによって提示されるID情報の一部であるスマートカードの固有の識別ストリング（または、識別ストリングは、スマートカードによって送られない場合には、このID情報に基づくデータベースから導出される）と組み合わせると変換後にはスマートカードに割り当てられたパスワードとなる単一のシードのみである。

【0046】d. スマートカードによって提示されるストリングは、常に、同一であるか、Oには事前には未知であるかのいずれかであるため、初期ストリング（ID, RND1）が記録の再生でないことを保証するために追加の認証ステップが所望されることもある。これは、Oが、例えば、そのIDとランダムストリングRND2とからなるチャレンジメッセージをSに送ることによって実現される。このストリングは、SがOにログインした後に送ることも可能であり、また、（図3のように）パスワード応答とともに送ることも可能である。SはSの「ルート」（一次ソース）パスワードでRND2を暗号化し、その結果のストリングK₁（RND2）をOへ転送する。

【0047】e. RND2ストリングに含まれるIDに基づいて、Sは、Oがユーザであると判定し、必要なキー（すなわち、Oのパスワード）を取得し、K₁（RND1）を復号する。復号の結果RND1となると、Sは、Oが真正であると判定する。

【0048】f. その後、SはSの「ルート」（一次ソース）パスワードでストリングRND2を暗号化し、その結果のストリングK₁（RND2）をOへ転送する。

【0049】g. OはK₁（RND2）応答を復号し、その結果のストリングがRND2である場合、OはSが正当であることに満足する。これでログインプロセスは終了し、OはSにプロンプトを提示し、サービスの要求を受ける準備ができた状態になる。

【0050】上記の「ログイン」プロセスは、アクセスしたいコンピュータが全ログインプロセスを制御するような周知のログインプロセスとは異なるように見えることに気づくかもしれない。そのような周知のログインプロセスでは、コンピュータはユーザの初期識別情報を要求し、次にパスワードを要求する。その初期識別情報に基づいて、コンピュータはどのパスワードが期待されるかを知る。一方、スマートカードは、（Oとの）通信を開始するという意味では制御されているように見える。しかし、初期識別情報を要求する（情報を得る）代わりに、スマートカードは、IDおよびRND1の形式で情報を提供する。これは、Oからの応答が初期識別情報な

のか、それとも、パスワードなのかという問題を引き起こす。これがパスワードであれば、Sはそのパスワードが正しいか否かをどのようにして知るのだろうか。その答えは、Oからの応答が3つの目的のために使用されるということである。Oは、（RND1に含まれるIDによって）初期識別情報の意味で自己を表示し、RND1を暗号化するために正しいキーを使用することによって自己を認証し、暗号化モードで返されるRND2によってSの正当性を問う。

【0051】Oがログインされると、Hは、サービス提供者（SP）によって提供されるサービスのインストールの要求を通信することができる。Oによってインストールされるよう要求された特定のサービスに関する通信は、人間との対話を含むこともあるが、自動化も可能である。例えば、Hは、所望されるサービスをSに通信し、SがOと通信することが可能である。図4に、サービスのインストールのためのプロトコルを示す。

【0052】a. Hはサービス要求をSに転送する。

【0053】b. Sはこの要求を暗号化し、それをOへ転送する。OとSの間の電子通信は、S内の公開キーの私的キー要素で暗号化可能である。Sはその公開キーをOに送っておく。あるいは、通信は、スマートカードの「共有秘密」でも暗号化可能である。「共有秘密」として「ルート」（一次ソース）パスワードを選択することが可能であり、または、一時的な「共有秘密」を（上記のように、公開キー暗号化を使用して）OからSへ提供することが可能である。図4では、「ルート」（一次ソース）パスワードを暗号化に使用して、要求ストリングK₁（REQ）を作成している。

【0054】c. 要求されたサービスを知ると、OはSPと交信し、SPがサービスをHに提供することに同意することを確認する。

【0055】d. サービスの提供がSPに同意されると、Oは一時的パスワードを選択し、そのパスワードをSPに（おそらくは暗号化通信によって）通知してから、S内にSPのためのディレクトリおよびパスワードファイルを作成する。

【0056】e. パスワードファイルがSPユーザのために設定されると、その一時的パスワードがSに（上記のように、暗号化通信によって）送られ、このディレクトリおよびパスワードファイルの所有権はSPに移転される（このパスワードは、将来のSPとの通信セッションにおいて「共有秘密」キーとして利用可能である）。また、SPが必要とするその他のアプリケーションソフトウェアはこのときにインストールすることが可能であり、Oがそれらのファイルを暗号化モードで送信する。あるいは、アプリケーションソフトウェアはOによってインストールされないようにも設定可能である。

【0057】f. この時点でHには、最終セットアップのためにSPと交信するよう通知される。

【0058】g. Hは、図3のようなログインシーケンスを使用して、ただし、暗号化キーとして一時的SPパスワードを使用して、SとSPの間の通信路を設定する。

【0059】h. SPへのログインが確立すると、Sはサービス要求を送出し、SPは応答して、新しいパスワードと、Oによってインストールされなかった必要なファイルと、データとをインストールする。これでサービスインストールは完了する。

【0060】「サービス提供者によるサービスの提供」上記のように、サービス提供者は、単に、スマートカードに割り当てられたディレクトリを有するユーザである。サービス提供者は、スマートカードのプロセッサ(P)がスマートカードとサービス提供者の間の通信を確立するとログインする。前のように、ログインプロトコルには3つの要素がある。

(1) SPは、PがHであることを確定したい。

(2) Sは、ログインするユーザが真のSPであることを判定したい。

(3) SPは、正当なSと通信していることを判定したい。

【0061】これらの3つの要素は、図3について説明したプロトコルで実行される。ログイン成功後にのみ、サービス要求を進めることができる。サービス要求は、例えば、HがSP(例えば銀行)に、Sの「電子財布」を満たすことにより、Sに「お金」をインストールすることを要求することである。電子財布の充填とは、例えば、単に、SPによって所有されるあるファイルにある値をインストールすることである。

【0062】「商人との対話」十分ゆとりがある場合、スマートカード保有者は、スマートカードとビジター(V)ユーザである商人とを対話させたいと思うことが予想される。上記の方式によれば、このような対話は2つの方法で可能である。1つは、スマートカードと商人との直接対話であり、もう1つは、スマートカード、商人、およびサービス提供者を含む三者間対話である。三者間対話方式のためのプロトコルは、図6に示すとおりであり、以下になる。

【0063】a. PはSとVの間に(SをVに渡すことによって、または、SをVにリモート接続することによって)通信を確立する。

【0064】b. Sは入力を促し、PはPINストリングを提示する。これが正しく一致すれば、Sは、PがHであると判定し、標準の「ログイン」シーケンスに進み、そのID情報およびRND1を送る。

【0065】c. VはSPとの通信路を設定し、SPに自己を表示し、ID情報およびRND1を中継する。

【0066】d. ID情報が与えられると、SPはそのパスワードを決定し、そのパスワードでRND1を暗号化する。その結果のストリングK₂(RND1)が、ラ

ンダムストリングRND2とともにSに送られる。

【0067】e. Sは、SPがK₂(RND1)を形成する際に正しいパスワードを使用したかどうかを判定し、その結論が真であれば、RND2を暗号化し、その結果K₂(RND2)をSPに転送する。

【0068】f. SPは、Sが正しいパスワードを使用してRND2を暗号化したことを確認すると、プロンプトをVに送り、商人に、Sの使用の要求に進むことができることを通知する。

【0069】g. VはSPからのアクション(例えば、SPにあるHの口座からある値を削除する、または、SにありSPによって所有されるファイルのある値を変更する)を要求する。

【0070】h. SPはその要求を満たし、必要であれば、SPパスワードで暗号化した適当なコマンドをSに送る。

【0071】スマートカードに商人(または、商人の銀行、もしくは、商人にサービスを提供し商人の代わりをする者と提携した商人)と直接対話させたい場合、スマートカードと事前に確立した関係を有しない者がスマートカードにログインすることを可能にするメカニズムを確立する必要がある。「ビジター」ユーザディレクトリがこの要求を満たし、このユーザはパスワードを有しない。結果として、ビジターユーザは非常にセキュリティのないユーザであるため、Vのアクセスは厳格に制御されなければならない。

【0072】例えば、解く必要のある1つの問題は、このようなビジターユーザが、商人によって指定されるサービス提供者のみのアプリケーションファイル(プログラム)にアクセスすることができるのか、それとも、すべてのサービス提供者のアプリケーションファイルにアクセスすることができるのか、ということである。すべてのサービス提供者のアプリケーションファイルへのアクセスが許可される場合、最も簡単な方式は、「ルート」(一次ソース)が、パスワードなしでビジターユーザディレクトリを設定し、ビジターユーザがオペレーティングシステムコマンドの制限されたセットのみを実行することを可能にする制限シェルを与えることである。すなわち、変数PATHを、「ルート」(一次ソース)によって所有される1つのディレクトリ(いくつかのオペレーティングシステムコマンドのみを含む)と、SPがビジターユーザに実行アクセスを許可したい実行可能ファイルを含むSPサブディレクトリ(またはサービス提供者/ユーザの選択したサブディレクトリ)とを含むように設定する。

【0073】指定したSPのみのアプリケーションファイルにアクセスを許可する場合は、もちろん、SPを指定しなければならず、指定したSPの実行可能ファイルのみを含む手段を設けなければならない。この場合も、これは制限シェルによって容易に実現され、PATH変

数は指定したSPのディレクトリ（または選択したサブディレクトリ）を含む。プロトコルは、図7に示すとおりであり、次のようになる。

【0074】 a. Sは入力を促し、PはPINストリングを提示する。これが正しく一致すれば、Sは、PがHであると判定し、標準の「ログイン」シーケンスに進み、そのID情報およびRND1を送る。

【0075】 b. Vは、パスワードを有しないため、単にストリングRND1を返す。

【0076】 c. この応答によって、Sは、ユーザがビ
ジターユーザであることを認識し、公開キーK_{pr}を送出
する。（公開キーは、ID情報の一部として既に送って
しまっていることも可能である。）この時点で、Sは、
公開キー、ID情報およびRND1を含むメッセージか
ら導出される「デジタル署名」を送ることもできる。
また、Sは、提案する「共有秘密」（図7には図示せ
ず）を構成する暗号化ストリングを送ることもできる。
提案した「共有秘密」およびデジタル署名はいずれも
公開キーで暗号化される。

【0077】 d. Mは、提供された公開キーを使用して
「デジタル署名」を解読する。解読した「デジタル
署名」が適当なストリングと一致した場合、VはRND
2を送出する。

【0078】 e. Sは、公開キーでRND2を暗号化
し、K_{pr}（RND2）によって応答する。

【0079】 f. Vは、このメッセージをK_{pu}で復号
し、RND2を取得した場合、Sと通信していることを
確定する。

【0080】 g. Vは、時刻および日付の情報を、K_{pr}
で暗号化してSに送り、Sはプロンプトを返す。

【0081】 h. Vは、同じくK_{pr}で暗号化して要求
（Vが求めるアクションおよび使用されるSPを識別す
る）をSに送信し、Sは、指定されたSPと交信する許
可によって応答する。この許可は、公開キーK_{pr}で暗号
化される。

【0082】 一般的に、商人は、商人によって提供され
る商品またはサービスと引き換えに、Hに属する資金を
得たいと考える。上記のように、銀行のようなサービス
提供者が、ある値を保持する「電子財布」をインストール
することは全く可能である。この値は、電子財布ファ
イルというファイル内にあり、サービス提供者によって
所有される。

【0083】 商人は、電子財布ファイルにアクセスした
いと考え、SP（Hと提携している）はこのファイルへ
のアクセスを許可するが、その許可は非常に制限され厳
格に制御されてのみなされる。このように、このファ
イルはすべてのログインしたユーザにとってアクセス可
能であるが、SPによってインストールされSPによって
所有されるコマンドを通じてのみそれは可能である。こ
のコマンドは、ファイル内の値から金額を差し引く（そ

の結果が負にならない限り）一時的な許可を他のユーザ
に与える。また、このコマンドは、ログファイルにその
取引を記録し、図7のように暗号化された許可ストリン
グを提示する。このように、SPは、オペレーティング
システムによって期待される規定の名前で電子財布ファ
イルを作成し、そのファイルに、ある値および特定のオ
ペレーティングシステムコマンド（これは「ルート」
（一次ソース）によって所有されない）を入れ、そのフ
ァイルにアクセスし、そのファイル内のその値から金額
を差し引く。

【0084】 図では、許可ストリングは、Sの公開キー
で暗号化されているが、これは、指定されたSPパスマ
ードで暗号化することも可能である。このストリング
は、商人がそれを単に何回か複製してその応答をSPに
送るということがないことを保証するように十分強固で
なければならない。これはいくつかの方法で実現するこ
とができる。それには、日付および時刻のタイムスタ
ンプを有すること、「電子財布」内の「前」および「後」
の値の表示、Sによって供給されるシーケンス番号、な
どが含まれる。この許可ストリングはVによって解読可
能でなく、従って、変更不能であるため、セキュリティ
は保持される。

【0085】 前述のオペレーティングシステムコマンド
に関して、そのようなコマンドの流れ図を図9に示す。
ブロック200で、コマンドは、ビジターユーザディレ
クトリ内の（規定された名前の）ファイルを参照するこ
とにより開始する。このファイルは、例えば改行文字に
よって区切られた4個のエントリを含まなければなら
ず、オペレーティングシステムは、この4個のエントリ
が、a) 日付および時刻と、b) 商人のID（例えば、
名前、住所、およびおそらくはコード）と、c) 差し引
く金額と、d) 使用する「電子財布」を有するサービ
ス提供者とからなると仮定する。

【0086】 このファイルが存在しない場合、または、
要求された数のエントリを有しない場合、制御はブロッ
ク210に移り、商人（ビジターユーザ）にこの不足を
通知する。ファイルが存在する場合、ブロック220
で、コマンドは、サービス提供者（SP）の電子財布フ
ァイル内の値を読み出す。ブロック230は、商人が引
き出したい金額が電子財布内の値より大きいかどうか評
価する。金額のほうが多い場合、制御はブロック24
0に移り、拒絶メッセージを構成しそれを商人に、およ
び、スマートカード内のログファイルに転送する。金額
が値より低い場合、制御はブロック250に移り、ログ
ファイルで、さまざまな不正の兆候がないかどうか検査
する。これは、実行中のコマンドによって呼び出される
別のコマンドとすることも可能である。図3に示すよう
に、ブロック250は、3種類の出力を生じる可能性が
ある。第1の出力は、潜在的な不正条件（例えば、この商
人は、事前に選択されている時間間隔内に規定の回数よ

り多くスマートカードを使用した)を示唆する。第2の出力は、SPによって提供され商人にSPと取引について協議させるしきい値ファイルに応答する。第3の出力は、標準状態を表示する。

【0087】潜在的な不正条件は、保有者のログファイルに格納されている情報によって処理され(ブロック260)、その後制御はブロック240に移る。格納されている情報は、商人、引き出そうとした額、拒絶理由などを識別する。これは、保有者に、カードの発行者/所有者と、および必要であれば政府当局と対話するのに必要な情報を提供する。必要に応じて、不正条件の疑いがあるときにスマートカードは無効にされる。

【0088】SPによって設定されたしきい値を超過した(例えば、SPが、1000ドルを超える引き出し許可を「リアルタイムで」求めた)場合、ブロック270でメッセージが構成され、制御はブロック280に移る。

【0089】ブロック280は、標準状態が示されたときにもブロック250から直接到達する。ブロック280は、スマートカードのログファイル内にあるシーケンス番号をインクリメントし、値ファイル内の金額から商人が要求する金額を差し引く。その後、ブロック290は、新しいシーケンス番号、日付および時刻、商人の識別情報、金額、およびSPからなるストリングを作成する。ブロック300は、ストリングのデジタル署名を作成し、ブロック310は、ブロック220で構成されたメッセージと、ブロック300で構成されたストリングと、デジタル署名とからなるメッセージを作成する。最後に、このメッセージが、商人に、および、スマートカードのログファイルに送られる。

【0090】商人の装置は2つのことのうちの1つを行う。SPと協議するようにとのメッセージが存在する場合、商人の装置はSPに接続され、ブロック310で作成されたメッセージを転送する。その後、商人は、金額に対する即時クレジットを得ることができる(もちろん、署名に基づいて、そのメッセージが正当であると結論される限り)。商人によって受信されたメッセージがブロック220によって構成されたメッセージを含まない場合、商人は単に、許可ストリングを格納し、選択された時間間隔(例えば就業日全体)にわたりこのような許可ストリングを収集し、その後、その許可ストリングを適当なSPに転送する。

【0091】許可ストリングはSの公開キーで暗号化されているように示されているが、指定されたSPのパスワードで暗号化することも可能である。許可ストリングは、商人が単にそれを所定回数複製してSPに送ることができないことを保証するように十分強固でなければならない。これはいくつかの方法で実現することができる。それには、日付および時刻のタイムスタンプを有すること、値ファイル内の「前」および「後」の値の表示を有

すること、Sによって供給されるシーケンス番号を有すること、などが含まれる。この許可ストリングはVによって解読可能でなく、従って、変更不能であるため、セキュリティは保持される。

【0092】[サービスセンタとしてのスマートカード発行者/所有者] 本発明の1つの特徴は、スマートカードの発行者/所有者(O)が、スマートカード上に存在する「アプリケーション」を有するサービス提供者の一般的知識を有し、そのサービス提供者を制御することである。第1に、Oはサービス提供者のディレクトリの設定を制御する。第2に、Oは、保有者の要求に応じて、または、Oがスマートカードにアクセスすることができるときには、(保有者の同意の有無に関わらず)任意のディレクトリを削除することができる。第3に、Oはスマートカードを共有するすべてのサービス提供者の識別情報と、それらのサービス提供者のさまざまな詳細を知る唯一の当事者である。第4に、オペレーティングシステムの設計を通じて、Oは、各サービス提供者がアクセスすることができるメモリの量を制御し、従って、スマートカード上に「共存」することが可能なサービス提供者の数を制御することができる。第5に、Oは特定の種類の取引に対してサービス提供者のグループ化を定義することができる。第6に、Oは、サービス提供者によって占有される空間に比例して、スマートカード上に存在する権利に対してそのような各サービス提供者に課金することができる。

【0093】上記のすべてのことから明らかなように、本発明の方式からいくつかの利益が生じる。例えば、その1つは、保有者がアクセスすることができる他のサービスについての知識を有するサービス提供者はないことである。もう1つは、任意のおよびすべてのディレクトリを削除する能力を有するのが、利害関係のない当事者、すなわちOであるということである。この当事者は、欠陥のあるカードを「修理」し、すべてのサービスを再インストールする能力も有する(所有者の代表的能力)。反対に、Oは、すべてのディレクトリを削除する能力を有し、この能力は、スマートカードが盗難にあったと判定されたときに執行される。

【0094】セキュリティに関しては、考慮する必要のある4つの形式の攻撃がある。第1は、侵入者が「ルート」(一次ソース)になろうとする場合である。第2は、侵入者がサービス提供者になろうとする場合である。第3は、当事者(「ルート」(一次ソース)、サービス提供者、侵入者、ピジター、保有者)が、許可されている以外のことをしようとする場合である。第4は、所持者が真正の保有者でない場合である。

【0095】第1の形式の攻撃に関しては、最初の主要な関門は「ルート」(一次ソース)パスワードである。これは、「ルート」(一次ソース)としてのログインが試みられたが失敗したときにオペレーティングシステム

がスマートカードを完全に無効にするように設定されるという意味で有効な関門である。例えば、すべてのディレクトリを消去することができる。

【0096】サービス提供者としてログインしようと試みることは、わずかにゆるい方法でのみ扱われるべきである。すなわち、カウンタが、サービス提供者としてログインしようとして失敗した試行を追跡するように設定することが可能である。試行失敗回数が事前に選択した値（例えば4）を超えた場合には、スマートカードは無効になる。このような状況では、スマートカードの無効を、攻撃の対象であったサービス提供者のディレクトリ10のみにすることも、「ルート」（一次ソース）ディレクトリ以外のすべてのサービス提供者ディレクトリにすることも可能である。

【0097】スマートカードとの最も多数の通信はビジターユーザによるものである。これらの通信はフレキシブルにする必要があるが、用心深いものである必要もある。UNIXオペレーティングシステムでは、PATHにないコマンドの実行に対しては親切なメッセージが出るが、スマートカードは、許されないコマンドにアクセスしようとするこれらの試行を監視する必要がある。この場合も、カウンタを使用して、事前に選択したカウントを超えた場合に、ビジターとの通信を終了し、メッセージをスマートカードに格納し、保有者以外の者に対してカードを無効にすることができる。保有者のディレクトリに格納されることになるそのメッセージは、中断した取引の詳細からなる。

【0098】もう1つのセキュリティ手段は、ビジターによる正当な取引にも関係することがある。上記のように、「ルート」（一次ソース）によって所有されるファイルのうちの1つにログファイルがあり、これはスマートカードによって実行されたすべての取引の記録を保持する。このファイルは、与えられた時間間隔に1つのビジターによってあまりに多くの取引があった場合、与えられた時間間隔にあまりに多くの取引があった場合などのような特定の状況が存在するようになるときに、特定のビジターユーザまたはすべてのビジターユーザを許可しないようにチェックすることが可能である。

【0099】スマートカードと通信する当事者はOKであるが、カードの所持者に問題がある場合には、わずかに異なるセキュリティ問題が生じる。この場合、スマートカードと対話している当事者は、その時点およびそれ以降では、スマートカードの使用を防止するのに協力したいと考えると容易に仮定される。これはいくつかの方法で実現される。例えばスマートカードが盗まれたものであるために、ログインシーケンス中に所持者によって提示されたIDが誤りである場合、商人は「ルート」（一次ソース）に属するファイルにメッセージを書き込むコマンドを実行しカードを無効にすることができる。この場合、カードを復元する唯一の方法は「ルート」40

（一次ソース）と通信することである。「ルート」（一次ソース）がそのメッセージを読んだ場合、所持者が実際は真の保有者であるか否かを判定し、適当なアクションをとることができる。

【0100】あるいは、商人の装置はスマートカードをカードの発行者／所有者に接続することも可能である。所有者はまずスマートカードを無効にしてから、スマートカードの所持者と対話して、その所持者がそのスマートカードを所持する権限を有するか否かを判定する。その所持者がその権限を有する場合、発行者／所有者はスマートカードを再び有効にする。

【0101】[スマートカードサービスの貯蔵所としてのサービスセンタ] スマートカードの上記の構造およびオペレーティングシステムが与えられると、スマートカード上のすべてのサービスをインストールする発行者／所有者がそれらのサービスの知識を有することは明らかである。すなわち、発行者／所有者は（スマートカードの「ルート」（一次ソース）所有者ではあるが）さまざまなサービス提供者によって所有されるファイル内を調べる能力を有しないが、それにもかかわらず、発行者／所有者は各スマートカード上にどのサービス提供者が存在するかについて知っている。この知識は、（各スマートカードが自分自身に関するそのような情報を保持することもできるが）発行者／所有者によって所有されるデータベースに保持することができる。

【0102】スマートカードを紛失または破損した場合、すべてのサービス提供者をインストールした新しいスマートカードを保有者に発行することができる。回復できない唯一の項目は、旧ファイル内にさまざまなユーザによって作成されたデータファイルと、サービス提供者のパスワードである。初期インストールについては、一時的なパスワードファイルのセットをインストールすることができる。その後、発行者／所有者はサービス提供者と通信して、一時パスワードについて通知し、保有者はサービス提供者と通信してそのパスワードを変更し、それぞれのディレクトリに必要なファイルを入れることができる。

【0103】[監査証跡] 上記のように、「ルート」（一次ソース）はログファイルを保持し、その中に各取引の記録を格納する。その後、このファイルは、保有者またはサービス提供者が課したいさまざまなしきい値を追跡するために使用することができる。

【0104】スマートカードの過度の使用は不正使用の表示の可能性がある。上記のように、このような使用は、ログファイルの注意深い監視によって検出することができ、それによって停止される。

【0105】しかし、ログファイルのもう1つの使用方法として、完全に正当な使用に関するものも可能である。例えば、クレジット提供サービス提供者は、すべての小さい取引に対しては商人から「バッチ」送信（おそらく

は就業日の終わりに)をさせながら、ある限界を超える負担を受ける場合には直ちに通知してもらうことができる。スマートカードの「電子財布」に関して、保有者は、スマートカード内の金額値がある限界を下回った場合に保有者の銀行と自動的に交信し、さらに追加の資金をスマートカードに振り替えるように命令することができる。

【0106】監査証拠のさらにもう1つの使用法は、紛争解決に関するものである。商人が、スマートカードがある商品またはサービスを取得するために使用されたと主張し、保有者がその主張を争う場合、ログファイルは、その紛争を解決するために使用することができる。

【0107】[サービス提供者間の協力] サービス提供者が協力的提携をすることも全く可能である。このような提携は、スマートカードがアクセスされるときはいつでも、または、スマートカードが特定のユーザによってアクセスされるときに、スマートカードで実行されるさまざまな活動を指定することができる。このような可能性の数は無制限であり、以下の例は単なる例示のためのものである。

【0108】例えば、会社Aが、ガソリンを頻繁に購入する必要がある巡回販売員を雇用しているとする。Aは、Oと交信して、各販売員(保有者)にスマートカードを発行させ、Aをサービス提供者として、および、Gをガソリン提供者としてインストールするようにOに要求する。しばらく後に、Aは、銀行Bと、販売員に対するクレジットの提供者として契約を結ぶ。このサービスは、例えばGの協力を得ることによって、販売員に属するすべてのスマートカードにリモートでインストールすることが可能である。

【0109】特に、Aは、スマートカードがGと対話し、AがユーザであるがBがユーザでないことを発見したときには、Oとの通信を要求するようインストールすることをGに要求することができる。Gがする必要があることは、HがGと通信するためにログインしたときに実行されるファイルを変更し、スマートカードがOを呼び出すようにすることのみである。

【0110】[POS環境でのスマートカードオペレーティングシステムの使用] 図10に、理解を容易にするためにいくつかのサブシステムに分割したスマートカードPOS配置を示す。第1のサブシステムは、携帯型スマートカード410であり、ユーザの情報を格納し交信することが可能なメモリを含む。第2のサブシステムは、スマートカードリーダ/ライタ415であり、これは、第3のサブシステムであるPOS端末418を連結する。このPOS端末418は、スマートカード内のメモリにアクセスするのに必要なアプリケーションソフトウェアを実行するコンピュータまたは専用ワークステーションからなる、適当に設定されたアプリケーションステーションである。アプリケーションソフトウェアは、

POS端末418のメモリ420内にあり、スマートカード410のメモリに格納された情報の取得および変更をすることができる。メモリ420は、例えば、ランダムアクセスメモリ(RAM)、読み出し専用メモリ(ROM)などよい。

【0111】スマートカード410は、オペレーティングシステムコマンドのセットを通じてアクセスされる実行可能オペレーティングシステムを実行する。それらのコマンドは、図2～図9について既に説明したように、カードセキュリティによって要求される規則に従って、カード上のファイルシステムを操作する。このオペレーティングシステムは、POS端末プロセッサ424上で実行可能なアプリケーションソフトウェアによって実現される。プロセッサ424は、当業者に周知の種類のマイクロプロセッサ装置でよい。

【0112】スマートカード410内にある主要な要素には、スマートカードプロセッサ4110、電氣的消去可能プログラマブル読み出し専用メモリ(EEPROM)4115、アナログインタフェース回路4130、変成器4120の二次巻線4121、および、容量性プレート4125～4128がある。

【0113】スマートカードプロセッサ4110は、中央処理装置と、ランダムアクセスメモリおよび読み出し専用メモリの形のメモリ装置とを有する。インテル社から入手可能な部品番号80C51というマイクロコンピュータを適当にプログラミングすることによってスマートカードプロセッサ4110として使用可能である。このプログラミングは当業者に周知である。その内部の読み出し専用メモリによって提供されるファームウェア制御下で動作して、スマートカードプロセッサ4110は、EEPROM4115に直接転送されるデータと、リーダ/ライタ415を通じてPOS端末418に転送されるデータとをフォーマットする。EEPROM4115全体またはその一部は、スマートカードプロセッサ4110の統合部分であることも可能であり、あるいは、別個の要素とすることも可能である。また、スマートカードプロセッサ4110は、リーダ/ライタ415を通じてPOS端末418から受信されるコマンドを解釈する。

【0114】スマートカード410内のEEPROM4115を使用することによって、許可ユーザは、許可されたアプリケーションステーションで、必要に応じて新しい異なるデータによって、カードのメモリセクション内のあるアプリケーションファイルを再プログラムすることができる。EEPROM4115はいくつかの供給元から入手可能であり、その多くは、ジェー・ロバート・ラインバック(J. Robert Lineback)による「EEPROMが売れ出す準備は完了したか(Are EEPROMs Finally Ready To Take Off?)」、Electronics、第59巻第7号(1986年2月17日)第40～41ページ、という

記事に記載されている。動作電源が加えられている間は、繰り返し、EEPROMにデータを書き込みこと、および、EEPROMからデータを読み出すことまたは消去することが可能である。動作電源が除かれると、EEPROM内のデータに対する変化は残り、スマートカード410に再び電源が入るとそれは取得可能である。

【0115】アナログインタフェース回路4130は、スマートカード410をリーダ/ライタ415にインタフェースする手段を提供する。このインタフェースは多くの機能を実行する。それには、リーダ/ライタ415からスマートカード410に結合される磁気エネルギーからの動作電源を供給することと、リーダ/ライタ415とスマートカード410内のスマートカードプロセッサ4110との間でデータを結合することが含まれる。スマートカード410を動作させるための電源は、変成器4120の二次巻線4121によって提供される誘導性インタフェースを通じてアナログインタフェース回路4130に要求される。この変成器は、スマートカード410内のこの二次巻線がリーダ/ライタ415内の一次巻線4122に物理的に接近して配置されると形成される。POS端末418は、リーダ/ライタ415とスマートカード410の両方の動作のための電源を供給する。

【0116】変成器4120は、変成器の一次巻線4122と二次巻線4121の間の結合を増大させるためにリーダ/ライタ415内にフェライトコア4123を含むことも可能である。結合効率をさらに増大させるために、カード内の二次巻線4121に付随して変成器4120内に第2のそのようなコア4124を含めることも可能である。大電力が利用可能で効率が問題ではないような装置では、これらのコアの一方または両方を省略することができる。クレジットカードに電力を結合するために変成器を使用することは、米国特許第4,692,604号(発明者:アール.エル.ピリングズ(R. L. Billings)、発行日:1987年9月8日)で提案されている。

【0117】スマートカード410へのデータ受信およびスマートカード410からのデータ送信は、アナログインタフェース4130に接続された容量性インタフェースによって提供される。この容量性インタフェースは、スマートカード410上の電極すなわちプレート4125~4128がリーダ/ライタ415内の対応する電極すなわちプレート4155~4158に物理的に接近して配置されるときに形成される4個のキャパシタからなる。これらのキャパシタのうちの2個は、リーダ/ライタ415からスマートカード410にデータを転送するために使用され、残りの2個は、スマートカード410からリーダ/ライタ415にデータを転送するために使用される。誘導性インタフェースと容量性インタフェースの組合せは、リーダ/ライタ415とスマートカ

ード410の間の完全な通信インタフェースを提供する。

【0118】リーダ/ライタ415内のいくつかの要素の構成は、スマートカード410内のものを機能的に反映したものである。そのような要素は、例えば、アナログインタフェース回路4140およびPOS端末プロセッサ424であり、後者はマイクロプロセッサとすることが可能である。さらに、リーダ/ライタ415は電源4162を有し、これは、変成器4120を通じてリーダ/ライタ415からスマートカード410に、電源を供給し、さらに、クロック信号を結合するために使用される。

【0119】アナログインタフェース回路4140は、リーダ/ライタ415をPOS端末プロセッサ424にインタフェースする。POS端末プロセッサ424は、電源4162の動作を制御し、この電源は、誘導的に電力をスマートカード410に転送するために使用される。POS端末プロセッサ424はメモリ420に接続される。メモリ420は、従来のランダムアクセスメモリ(RAM)装置、読み出し専用メモリ(ROM)、消去可能プログラマブル読み出し専用メモリ(EPROM)などであり。

【0120】POS端末プロセッサ424は従来のUPCバーコードリーダ426の動作を制御する。バーコードリーダ426としての使用に適した装置は、例えば、米国特許第5,155,343号(発明者:チャンドラー(Chandler)他、発行日:1992年10月13日)、米国特許第5,124,537号(発明者:チャンドラー(Chandler)他、発行日:1992年6月23日)、および米国特許第5,079,412号(発明者:スギヤマ(Sugiyama)、発行日:1992年1月7日)に記載されている。いくつかの従来のUPCバーコードリーダ426は統合されたPOS端末プロセッサ426を有するが、他の従来のUPCバーコードリーダ426には、単に、光学的なUPCバーコードを、マイクロプロセッサによって解釈可能なデジタルデータストリームに変換するものもある。

【0121】UPCバーコードリーダ426は、従来のUPCバーコードを読み取る。このUPCバーコードは現在では、食料品、建材、電子製品、健康用品、雑誌、書籍などのさまざまな消費者商品に貼付され、または、印刷されている。商品428は、UPCバーコードを有するこのようなある消費者商品を代表する。UPCバーコードは、特定の商品または商品種別を識別するために使用される。従来のUPCバーコードの特徴は当業者には周知である。

【0122】図11に、EEPROM4115内に格納されスマートカード410によって使用されるデータ構造を示す。1つ以上のアプリケーション識別子1109、1110、1111が利用される。各アプリケーション

ョン識別子1109、1110、1111はそれぞれ口座識別子1114、1116、1117を含み、口座識別子は、与えられた口座を一意的に指定する。各口座識別子1114、1116、1117はそれぞれ口座残高フィールド1101、1103、1105を有し、これらのフィールドはそれぞれ口座残高を表す数値を格納している。オプションの個人識別番号レジスタ1107は、スマートカードユーザが保有する個人識別番号(PIN)に対応する数値を格納している。オプションの割引識別子1112、1115は、さまざまな購買に割引を適用するために利用可能である。

【0123】各アプリケーション識別子1109、1110、1111は、POS端末418のメモリ420に格納された1つ以上の特定の商品表の使用を指定する。(メモリ420の構造は後で図12を参照して説明する。)このようにして、アプリケーション識別子は、対応する商品表に特定の口座を割り当てる。例えば、第1アプリケーション識別子1109は2つの商品表識別子1118、1120を含み、これらはそれぞれ「商品表III使用」および「商品表IV使用」を指定する。各口座識別子1114、1116、1117は、1つ以上の対応する商品表識別子と関連しており、それぞれフィールド1118、1120、1122、および1124として図示されている。フィールド1118は商品表IIIの使用を指定し、フィールド1120は商品表IVの使用を指定する。

【0124】図11のアプリケーション識別子としてこれ以外のデータ構造も可能である。注意すべき点は、詳細は図12を参照して後で説明するが、商品表自体が各商品識別子に対応する口座に関係づけるものであるため、特定の口座に対応する商品表に関係づける必要がないことである。アプリケーション識別子が特定の口座を直接指定しない場合、この識別子は単に1つ以上の商品表識別子を含むのみである。例えば、第nアプリケーション識別子1111を考えると、口座識別子すなわち口座「n」1117および口座「n」の口座残高フィールド1105は削除され、商品表識別子1124のみが残ることになる。その結果、アプリケーション識別子は図12の表I(1211)および表II(1213)のデータ構造を有する商品表識別子とともに使用されることになる。しかし、この結果のアプリケーション識別子は、表IIIまたはIV(1215、1219)とともに使用されない。

【0125】オプションの割引識別子フィールド1112は、カード保有者が、例えば、高齢者割引、得意様割引、特別販売促進商品割引などのような資格がある場合の1つ以上の特別割引を指定するために利用される。割引は、割引識別子フィールド1112に指定された口座から引き落とされるすべての商品に適用することが可能である。あるいは、割引識別子フィールド1112は1

つ以上の商品表(例えば、表I、表IIなど)を指定することも可能である。

【0126】図12に、本発明の好ましい実施例によるPOS端末メモリによって使用されるデータ構造を示す。このメモリは、商品表I(1211)、商品表II(1213)、商品表III(1215)、および商品表IV(1219)のような複数の商品表を含む。各商品表1211、1213、1215、1219は、それぞれ、商品表識別子1201、1203、1207、1209を有し、これらは特定の商品表を一意的に識別する。また、各商品表1211、1213、1215、1219は商品のリストを含む。例えば、表III(1215)は、商品1000、商品1003、商品1004、および商品1005を指定するリストを含む。表IV(1219)は、商品1010、商品1012、商品1002、商品1001、および商品1011を指定するリストを含む。これらの商品1000~1005、1010~1012は、例えば、消費者商品を表す。特に、例えば、商品1000は特定のブランドのシャンプーを表し、商品1001はある種の製品を表し、商品1002は特定の朝食シリアルを表し、商品1003は長いベンチを表し、商品1004は緑色のカーディガンセーターを表す。

【0127】商品表IIIおよびIV(それぞれ1215、1219)は、商品のリストを含む。商品表1215、1219は、アプリケーション識別子1109、1110、および1111の場合のように、図11のデータ構造を有するアプリケーション識別子とともに使用される。しかし、商品表IおよびII(それぞれ1211および1213)のように、オプションとして、商品には特定の口座が関係づけられることもある。例えば、商品表I(1211)は、商品1000を口座Aに関係づけ、商品1001を口座Bに関係づける。このようにして、商品1000が購入されると、口座Aから商品1000の代金が引き落とされ、商品1001が購入されると、口座Bから商品1001の代金が引き落とされる。商品表自体が、与えられた口座を与えられた商品に関係づける場合、図11に関して既に述べたように、このような商品表の使用を指定するアプリケーション識別子は、口座識別子を含まない。例えば、表IおよびII(それぞれ1211、1213)のデータ構造は、特定の口座を指定しないが表識別子を含むアプリケーション識別子とともに使用される。口座識別子が存在する場合、端末プロセッサはそれを無視するようにプログラムされる。

【0128】図13に、本発明の好ましい実施例によって実行される動作シーケンスを説明する流れ図を示す。プログラム制御はブロック100から開始する。ブロック106で、プログラムは、消費者によって購入される特定の商品、例えば、商品1003(図12)、に対す

る実行を開始する。ブロック108で、プログラムは、商品1003が第1の口座、例えば、口座A(図12)から引き落とすべきか否かをチェックする。この作用は、POS端末メモリ420に格納され、スマートカードEEPROM4115に格納された1つ以上のアプリケーション識別子1109、1110によって指定される商品表(図12)を参照して実行される。口座A(図12)は、例えば、WICとして一般に知られているプログラムのような福祉プログラムを表すことも可能である。商品1003が口座Aから引き落とされるべきである場合、プログラムは、商品1003の代金をまかなうのに十分な残高が口座Aに残っているかどうかをチェックする(ブロック112)。不十分な口座残高しかない場合、プログラム制御はブロック116(その実行する作用は後述)にジャンプする。十分な口座残高が口座Aに存在する場合、プログラムは商品1003の代金を口座Aから差し引き、プログラム制御はブロック106にループバックし、そこでプログラムは購入する次の商品(そのような商品が存在すれば)について再び実行される。

【0129】商品1003が口座Aから引き落とされるべきでない場合、ブロック108からのNOの分岐によってブロック116へ進み、そこで、プログラムは、商品1003が口座Bから引き落とされるべきかどうかをテストする。図13の例では、口座Bはフードスタンプ口座を表す。商品が口座Bから引き落とされるべきでない場合、プログラム制御はブロック126(詳細は後述)にジャンプする。商品が口座Bから引き落とされるべきである場合、プログラムはブロック120に進み、そこで、口座Bに十分な口座残高があるかどうかを確認するテストを実行する。十分な口座残高がない場合、プログラムはブロック126(後述)にジャンプする。口座Bに十分な口座残高がある場合、プログラムはブロック122に進み、そこで、商品の代金が口座Bから差し引かれる。その後、プログラムはブロック106にループバックし、そこで、次の商品がもしあれば処理される。

【0130】ブロック116および120からのNOの分岐はブロック126につながる。實際上、ブロック126は、与えられた商品を購入したいが、その商品について引き落とす口座には不十分な口座残高しか存在しない場合に到達する。ブロック126の手続きによって、例えば現金、小切手、ビザ、マスターカード、ディスカバー、またはATMカードのような代替りの資金源からの商品の購入が可能となる。購入者は、さまざまな支払方法のメニューを提示され、利用可能な選択肢からある方法を選択することが可能である。

【0131】図13の流れ図は2つの口座(口座Aおよび口座B)を示しているが、本発明の方法は任意の都合の良い数の口座に適用可能である。上記の例に記載した口座は福祉プログラムに関するものであるが、通常のビ

ず、マスターカード、ディスカバー、または他のクレジットカード口座や、銀行、相互銀行、信用組合などを通じて得られる普通預金口座や当座預金口座のような他の種類の口座を利用することも可能である。

【0132】図14に、本発明の好ましい実施例によって実行される動作シーケンスの流れ図を示す。この動作シーケンスは、一般的に、消費者が購入のために1つ以上の商品を選択した後に、POS端末418(図10)で実行される。POS端末418(図10)は、一般的に、スーパーマーケット、食品雑貨店、またはデパートの勘定台に設置される。消費者商品には、例えば、朝食シリアル、箱、オレンジジュースの箱、シャンプーの瓶、洗濯洗剤、プラスチック製ごみ袋、冷凍チキン、およびいくつかの棒キャンディが含まれる。

【0133】ある種の消費者に関しては、従来のPOS端末の使用は問題を生じる。例えば、福祉受給者である消費者の場合、福祉プログラムはある特定の商品の代金をまかなうが、他の商品は考慮から除外する。WICという福祉プログラムは、「扶養家族」(すなわち、一般的に、青少年)の健康および福祉に書くことのできない食料品その他の商品の代金をまかなうように設計されていると仮定する。しかし、WICプログラムは、ある非本質的なすなわち贅沢な商品を排除するように慎重に設計され、福祉受給者が不要な、むだな、または有害な商品にプログラム利益を浪費する自由を有しないようにしている。WICプログラム受給者は、基本的な生活必需品をまかなうために利益を使用するように強制される。従って、WICプログラムは、上記の例では、オレンジジュース、朝食シリアル、および洗濯洗剤の代金はまかなうことになるが、棒キャンディの代金は不要な「贅沢品」として排除する。さらに、消費者によって洗濯される特定のブランドのシャンプーは比較的高価であり、福祉プログラムはある一定の金額までのシャンプーの代金しかまかなわないように調整されていると仮定する。現在のPOS端末では、消費者または勘定カウンターの店員が、福祉適格商品を他の商品から分離しなければならない。さらに、その商品を分離した後、さまざまな福祉プログラムの利益を調整するために追加の計算が必要となる。これらのステップは不要な遅延を生じ、勘定カウンターの店員の効率を低下させ、消費者が福祉適格商品について、または、非適格商品についてよく知らない場合、誤りを生じる。

【0134】前段落で説明した現在のPOS端末の欠点は、福祉プログラムに特有のものではない。例えば、非福祉消費者が、食料品にのみにはクレジットカードを使用して支払い、非食料品には現金で支払いたいことがある。同様に、消費者は、ある種の商品を購入するのに第1のクレジットカードを使用し、別の種類の商品を購入するのに第2のクレジットカードを使用したいことがある。近所のマーケットで夫婦で買い物をする場合に、各

人が自分のクレジットカードを有するとき、その夫婦は、ある商品の代金は半々に分け、同時にある商品の代金は全部一方の口座のみに負担させるようにしたいことがある。このようなことは、夫婦で別々のPOS取引を使用しなければ、現在のPOS端末を使用して実行することは不可能である。

【0135】現在のPOS端末の上記の制限および欠点は図14の動作シーケンスを実行することによって克服される。図14の動作シーケンスはブロック1500から開始し、そこでは、購入する商品の単一のセットを構成する複数の消費者商品がPOS端末に集められる。次に、消費者のスマートカードがPOS端末のスマートカードリーダ415（図10）によって読み取られる（図14、ブロック1502）。ブロック1504で、データファイルは、スマートカードメモリ（すなわち、図10のEEPROM4115）から端末プロセッサ424（図10）にアップロードされる。このデータファイルには図11のアプリケーション識別子1109、1110、1111が含まれる。スマートカードメモリから受信したアプリケーション識別子に応答して、端末プロセッサは端末メモリから1つ以上の商品表（図12、1211、1213、1215、1219）を取得する。各商品表は、スマートカードメモリからアップロードされたアプリケーション識別子で指定された口座が関係づけられる（図14、ブロック1506）か、または、スマートカードからアップロードされた商品表識別子が、POS端末プロセッサによって使用される口座および商品表を決定する。

【0136】ブロック1508で、端末プロセッサは、商品表が複数の口座に関係づけられているか否かを確かめるテストを、端末メモリから取得した各商品表に対して実行する。与えられた商品表が複数の口座に関係づけられている場合、プログラム制御はブロック1510に進み、そこで、POS端末プロセッサは、引き落とし優先アルゴリズムを実行して、ブロック1506で端末メモリから取得した商品表に関係づけられた複数の口座の間での引き落とし額の配分を決定する。この引き落とし優先アルゴリズムは、特定のシステムアプリケーションの必要を満たすように設計され、1つの商品が複数の口座に対応する場合の衝突を解決する作用を実行する。例えば、あるアプリケーションに適した引き落とし優先アルゴリズムでは、第1の口座と第2の口座がいずれも与えられた商品に関係づけられている場合、この商品は、十分な残高が第2の口座に存在する限り、常に第2の口座を使用して代金が支払われる。しかし、第2の口座が、その商品の代金をまかなうのに十分な残高を有しない場合、第1の口座から引き落とされる。別のアプリケーションに適した引き落とし優先アルゴリズムでは、第1の口座と第2の口座がいずれも与えられた商品に関係づけられている場合、この商品の代金は、50:50ま

たは60:40のような一定の引き落とし比率を使用して、口座間で比例配分される。ただし、以上の引き落とし優先配分アルゴリズムの例は単なる例示のためのものである。他の引き落とし優先配分アルゴリズムの特徴、構造、および動作は、当業者の知識の範囲内にある。

【0137】ブロック1512には、ブロック1508のNOの分岐から、または、ブロック1510の動作が実行された後に到達する。ブロック1512で、端末プロセッサは、商品識別装置、すなわち、UPCバーコードリーダ426（図10）を起動する。商品識別装置は、購入する商品の単一のセット内のある商品から商品識別子を取得する（図14、ブロック1514）。ブロック1516で、端末プロセッサは、ブロック1514で商品識別装置によって取得された商品識別子と同一の商品識別子を、ブロック1506で取得されたすべての商品表にわたって検索する。

【0138】ブロック1520で、端末プロセッサが商品識別子の1つ以上の一致を発見したかどうかを確かめるテストを実行する。発見しなかった場合、プログラム制御はブロック1522に進み、そこで、残余口座からその商品の代金が引き落とされる。この残余口座は、商品識別装置によって識別されたがブロック1506で端末プロセッサによって取得されたいずれの商品表にもリストされていない商品を追跡するために使用される。購入するすべての商品が識別された後、例えば、端末プロセッサとインタフェースするキーパッドのようなPOS端末入力装置を使用して口座を選択することによって、顧客の口座のうちの1つから残余口座の合計残高を引き落とすことができる。あるいは、残余口座残高の支払をするために、POS端末プロセッサは、（1）顧客の最高残高を有する口座から引き落とすこと、（2）POS端末入力装置からは、ある口座からの引き落としのみを許容し、他からの引き落としは許容しないこと、（3）顧客による現金支払いを可能にすること、ができるようにプログラムされる。

【0139】ブロック1522で、残余口座が引き落とされた後、プログラム制御はブロック1530に進み、そこで、購入のために提示する商品のセットのうちにPOS端末には他の商品があるか否かを確かめるテストを実行する。このような商品がない場合、プログラムは終了する。このような商品がある場合、プログラムはブロック1516に戻ってループする。

【0140】ブロック1520からのYESの分岐はブロック1524につながり、そこで、商品識別子にただ1つの一致があるかどうかを確かめるテストを実行する。ただ1つの一致がある場合、プログラム制御はブロック1528に移り、そこで、一致した商品識別子を含む表に関係づけられた口座が引き落とされる。この口座は、代金表に示された商品の代金を引き落とされる。この口座の残高が、商品の代金をまかなうには不十分であ

る場合、残余口座から引き落とされる。商品の代金は、この時点で、端末プロセッサからスマートカードプロセッサにダウンロードすることが可能である。あるいは、アプリケーション識別子の一部として口座残高がスマートカードからPOS端末にアップロードされたという事実により、端末プロセッサは、各商品が商品識別装置によって識別されると、商品ごとに、アップロードされた口座残高から商品代金を差し引くことも可能である。この減算は、POS端末内で行われる。最後の商品が商品識別装置によって識別されると、新しい口座残高が端末

10 プロセッサからスマートカードプロセッサにダウンロードされる。ブロック1528の動作を実行した後、プログラムは上記のブロック1530に進む。

【0141】ブロック1524からのNOの分岐はブロック1526につながり、そこで、前述の引き落とし優先アルゴリズムを実行して、一致する商品識別子を含む表に関係づけられた複数の口座の間で商品の代金を配分する。その後、プログラムは上記のブロック1530に進む。

【0142】

20 【発明の効果】以上述べたごとく、本発明によれば、スマートカード上に記憶された複数の口座のうちの任意の口座から引き落としすることによって1組の消費者商品を購入することが可能となる。

【図面の簡単な説明】

【図1】UNIXオペレーティングシステムの構造の図である。

【図2】スマートカードオペレーティングシステムのツリー構造の図である。

30 【図3】スマートカードとその発行者／所有者の間のログインプロトコルの図である。

【図4】スマートカード、その発行者／所有者およびサービス提供者に関わるプロトコルの図である。

【図5】スマートカードがサービス提供者からサービスを取得するプロトコルの図である。

【図6】スマートカード、ビジターユーザおよびサービス提供者に関わるプロトコルの図である。

【図7】サービス提供者への接続のない、スマートカードとビジターユーザの間のプロトコルの図である。

40 【図8】電気通信ネットワークを使用してスマートカードをリモート発給する配置の図である。

【図9】サービス提供者のファイルに記憶された値を引き出すオペレーティングシステムコマンドの流れ図である。

【図10】本発明の好ましい実施例の特徴を説明するハードウェアブロック図である。

【図11】本発明の好ましい実施例によるスマートカードによって使用されるデータ構造の図である。

50 【図12】本発明の好ましい実施例によるPOS端末メモリによって使用されるデータ構造の図である。

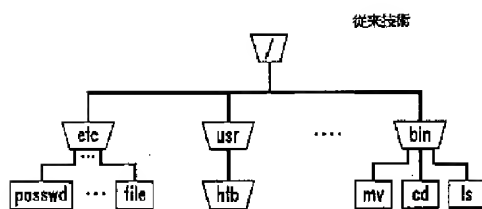
【図13】本発明の好ましい実施例の特徴を説明する流れ図である。

【図14】本発明の好ましい実施例によって実行される動作シーケンスの流れ図である。

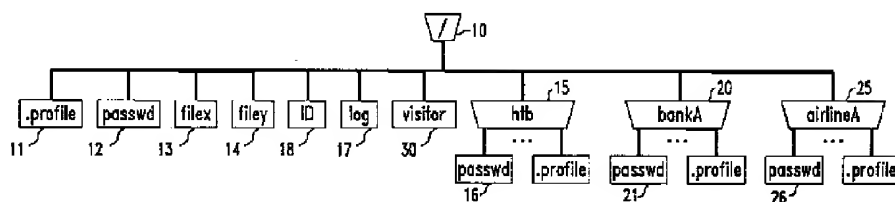
【符号の説明】

1101	口座残高
1103	口座残高
1105	口座残高
1107	個人識別番号レジスタ
1108	個人識別番号レジスタ
1109	アプリケーション識別子
1110	アプリケーション識別子
1111	アプリケーション識別子
1112	割引識別子
1114	口座識別子
1115	割引識別子
1116	口座識別子
1117	口座識別子
1118	商品表識別子
1120	商品表識別子
1122	商品表識別子
1124	商品表識別子
1201	商品表識別子
1203	商品表識別子
1207	商品表識別子
1209	商品表識別子
1211	商品表I
1213	商品表II
1215	商品表III
1219	商品表IV
410	携帯型スマートカード
4110	スマートカードプロセッサ
4115	電氣的消去可能プログラマブル読み出し専用メモリ (EEPROM)
4120	変成器
4121	二次巻線
4122	一次巻線
4123	フェライトコア
4124	フェライトコア
4125	容量性プレート
4155	容量性プレート
4130	アナログインタフェース回路
4140	アナログインタフェース回路
415	スマートカードリーダー/ライター
4162	電源
418	POS端末
420	端末メモリ
424	端末プロセッサ
426	UPCバーコードリーダー
428	商品

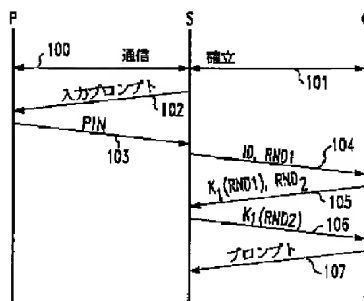
【図 1】



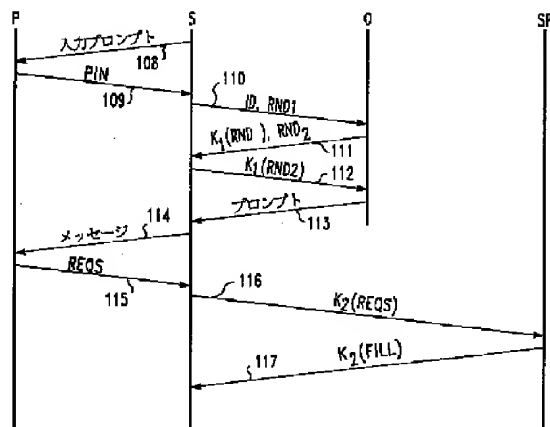
【図 2】



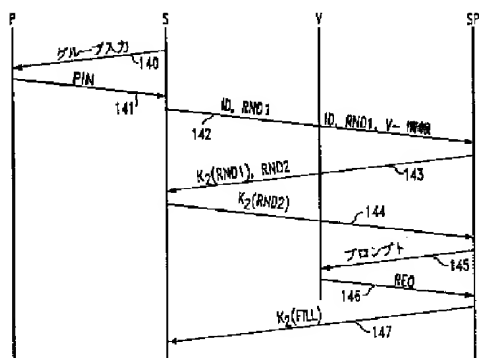
【図 3】



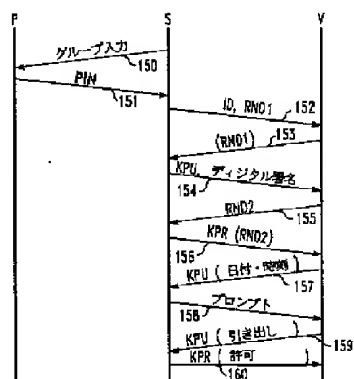
【図 5】



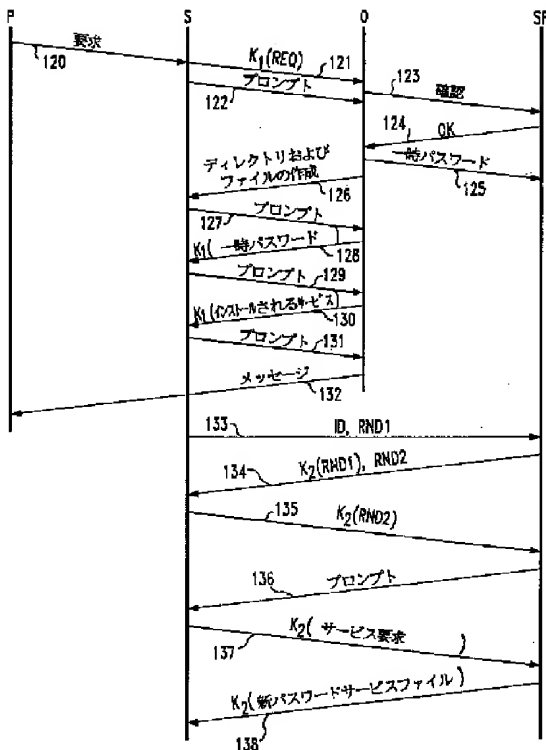
【図 6】



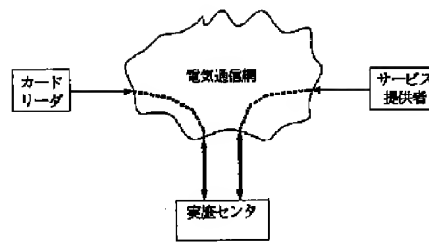
【図 7】



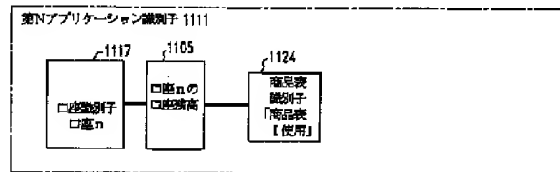
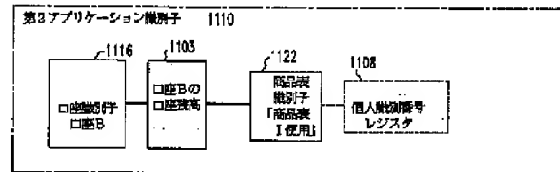
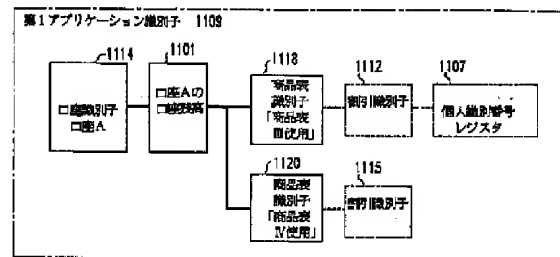
【図4】



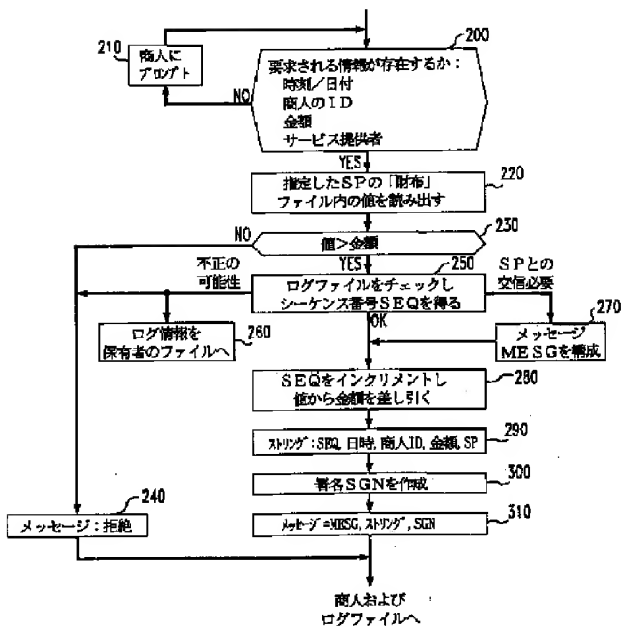
【図8】



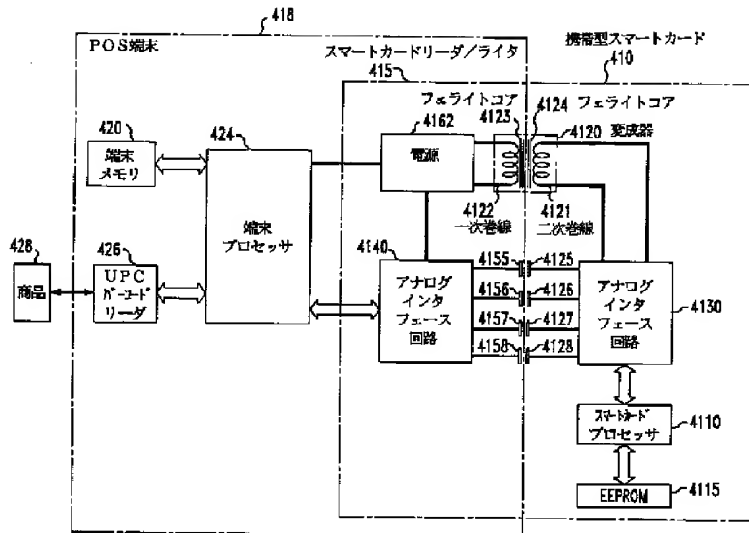
【図11】



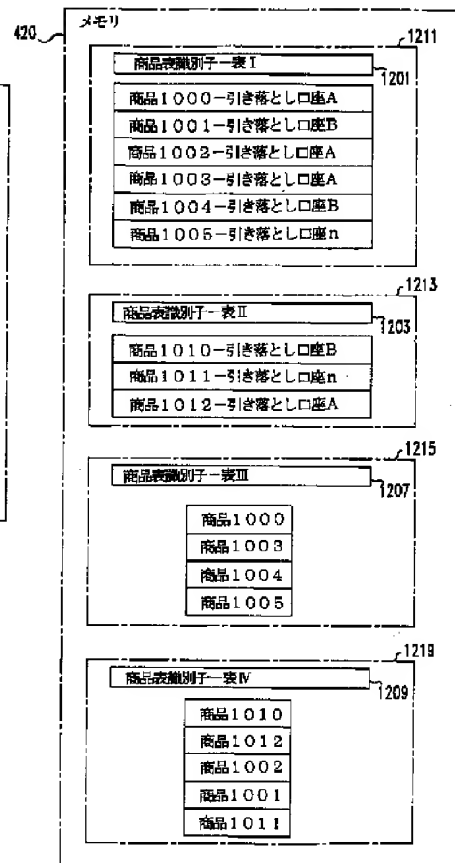
【図9】



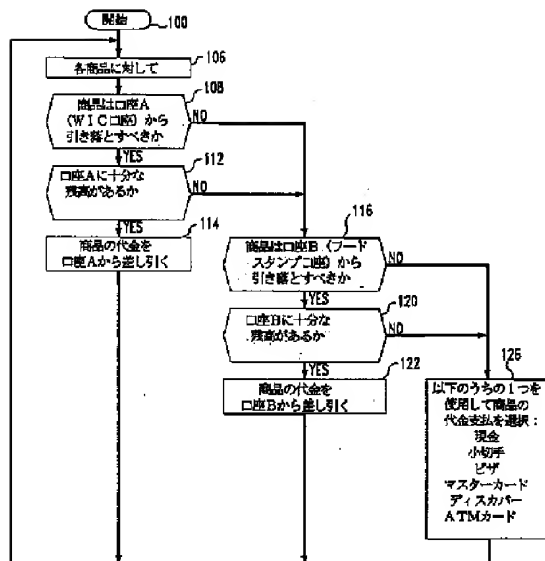
【図10】



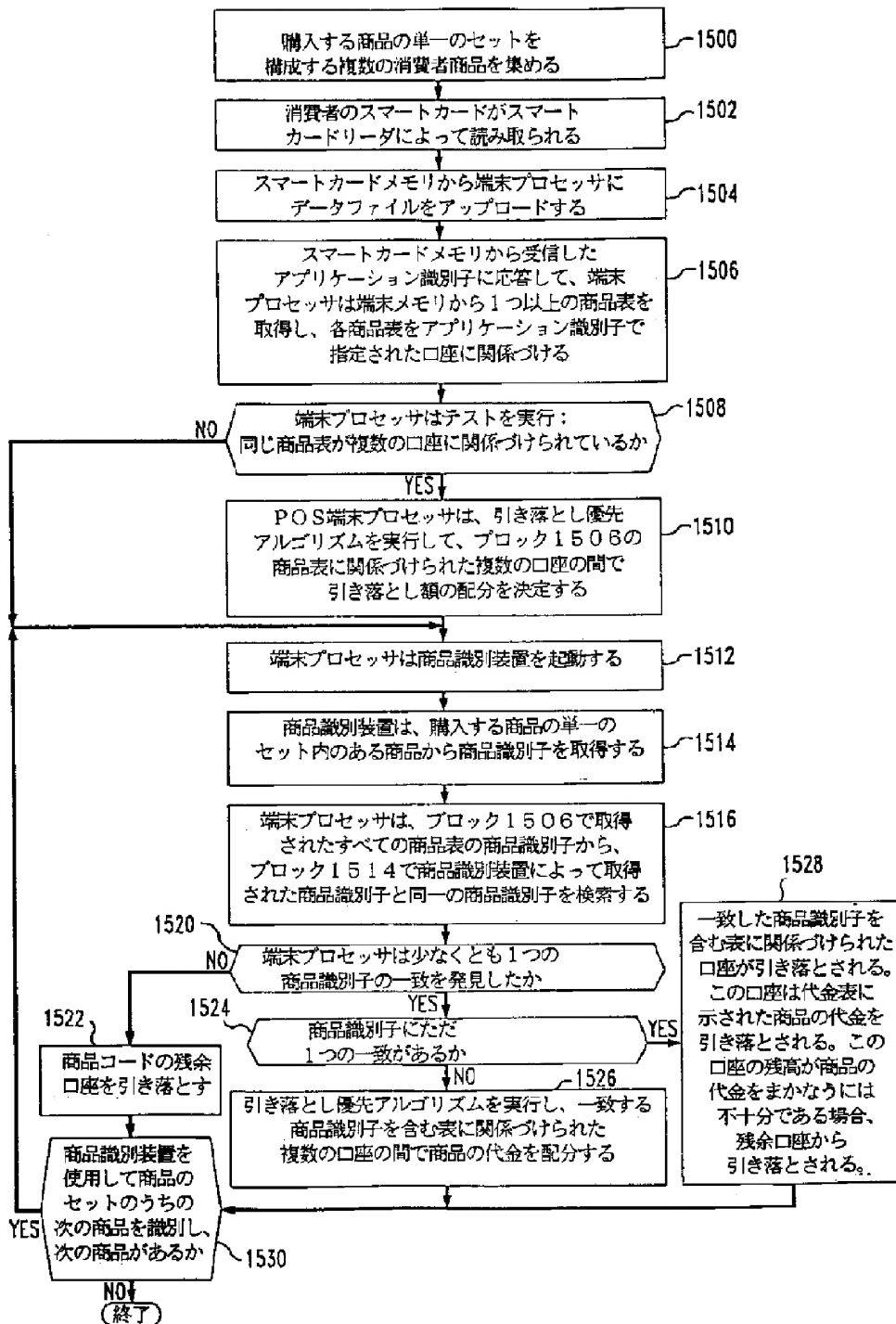
【図12】



【図13】



【図14】



フロントページの続き

(72)発明者 リディア アン カーティス
アメリカ合衆国、ニュージャージー、ブリ
ッジウォーター、ドゥーリトル ドライブ
1308

(72)発明者 キャサリン エム. マーフィー
アメリカ合衆国、ニュージャージー、ベッ
ドミンスター、ウッド ダック ポンド
ロード 17

(72)発明者 リチャード ジョン スキボ
アメリカ合衆国、ニュージャージー、スキ
ルマン、ドーランド ファーム コート
16